

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

In re: Equifax, Inc. Customer
Data Security Breach Litigation

This document relates to:

FINANCIAL INSTITUTION ACTIONS

MDL Docket No. 2800
No. 1:17-md-2800-TWT

Chief Judge Thomas W. Thrash, Jr.

**FINANCIAL INSTITUTION PLAINTIFFS' MEMORANDUM OF LAW IN
OPPOSITION TO DEFENDANTS' MOTION TO DISMISS THE
FINANCIAL INSTITUTIONS' CONSOLIDATED AMENDED
COMPLAINT**

TABLE OF CONTENTS

INTRODUCTION	1
FACTUAL BACKGROUND.....	4
ARGUMENT AND CITATION OF AUTHORITY	9
I. Plaintiffs Have Article III Standing.....	10
A. Plaintiffs Suffered Injuries-in-Fact Traceable to the Equifax Data Breach.....	10
1. Plaintiffs Suffered Injuries-in-Fact	10
a. The Compromise of the Credit Reporting and Verification System Constitutes an Injury to All Plaintiffs.....	11
b. Federal Law Required All Plaintiffs to Take Action in Response to the Data Breach.	13
c. FI Card Plaintiffs Have Suffered Additional Injuries	15
d. The Most Consequential Data Breach in History Has Exposed All Plaintiffs to a Substantial Risk of Fraudulent Banking Activity.....	17
2. Plaintiffs’ Injuries Are Traceable to the Equifax Data Breach.	21
B. The Association Plaintiffs Have Article III Standing	22
1. The Association Plaintiffs Allege Diversion of Resources	23
2. The Association Plaintiffs’ Equitable Claim Does Not Require Member Participation.....	23
II. Plaintiffs State a Claim for Negligence	25
A. Equifax Had a Duty to Plaintiffs	25
1. Equifax Had a Duty Not to Subject Plaintiffs to an Unreasonable Risk of Harm.....	25
2. Equifax Voluntarily Assumed a Duty to Handle Plaintiffs’ PII	

	& PCD with Reasonable Care.....	34
B.	Plaintiffs Alleged Causation and Damages.....	35
C.	The Economic Loss Rule Does Not Apply	37
III.	Plaintiffs State a Claim for Negligence Per Se.....	38
A.	Section 5 and Similar State Statutes Provide a Basis for Plaintiffs’ Negligence Per Se Claim.....	40
B.	The GLBA with the Safeguards Rule Provides a Basis for Plaintiffs’ Negligence Per Se Claim.....	43
IV.	Plaintiffs State a Claim for Negligent Misrepresentation	47
V.	Plaintiffs Adequately Allege Their State Statutory Claims.....	52
A.	Plaintiffs Can Constitutionally Bring Non-Georgia Statutory Claims against Equifax	52
B.	Equifax Misstates the Elements Required for the Statutory Claims at Issue.....	55
1.	Plaintiffs’ Statutory Claims Based on Equifax’s Unfair Conduct Need Not Meet All the Elements of Fraud	55
2.	Plaintiffs’ Statutory Claims Based on Equifax’s Deceptive Conduct Need Not Meet All the Elements of Fraud.....	57
a.	Plaintiffs Meet the Heightened Pleading Standard to the Extent Required	59
b.	Plaintiffs Adequately Allege Scier to the Extent Required.....	60
c.	Plaintiffs Adequately Allege Reliance to the Extent Required.....	62
3.	Plaintiffs Adequately Allege Injury	62
4.	Equifax Mischaracterizes Plaintiffs’ Equitable Claims	62
5.	Plaintiffs Qualify as “Consumers”	63
6.	State-Law Class Action Bans Are Unenforceable.....	64

C.	Equifax’s Claim-Specific Arguments Lack Merit	64
1.	<i>McConnell III</i> Is Irrelevant to Plaintiffs’ GFBPA Claim	64
2.	Plaintiffs Can Enforce a Massachusetts Ch. 93A Claim	65
3.	Plaintiffs Adequately Allege the MPCSA Claim	66
VI.	<i>Schnuck Markets</i> Is Inapposite	66
VII.	Plaintiffs Adequately Allege Their Entitlement to Equitable Relief	68
CONCLUSION		70

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Action Marine, Inc. v. Cont’l Carbon Inc.</i> , 481 F.3d 1302 (11th Cir. 2007)	36
<i>Adams v. Cong. Auto Ins. Agency, Inc.</i> , 65 N.E.3d 1229 (Mass. App. Ct. 2016), <i>review denied</i> , 86 N.E.3d 243 (Mass. 2017)	65
<i>Aetna Life Ins. Co. of Hartford, Conn. v. Haworth</i> , 300 U.S. 227 (1937)	69
<i>Allstate Ins. Co. v. Hague</i> , 449 U.S. 302 (1981)	53
<i>Am. Casual Dining, L.P v. Moes’ Southwest Grill, L.L.C.</i> , 426 F. Supp. 2d 1356 (N.D. Ga. 2006)	48
<i>Arcia v. Fla. Sec’y of State</i> , 772 F.3d 1335 (11th Cir. 2014)	22, 23
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	9
<i>Atlanta Nat. Bank v. Bateman</i> , 94 S.E. 853 (Ga. Ct. App. 1918)	30, 38
<i>Atwater v. Nat’l Football League Players Ass’n</i> , No. CIV 1:06CV1510 JEC, 2007 WL 1020848 (N.D. Ga. Mar. 29, 2007)	48
<i>Bailey v. Wheeler</i> , 843 F.3d 473 (11th Cir. 2016)	19, 22
<i>Ballenger Paving Co. v. Gaines</i> , 499 S.E.2d 722 (Ga. Ct. App. 1998)	33

<i>Bans Pasta, LLC v. Mirko Franchising, LLC</i> , No. 7:13-cv-00360, 2014 WL 637762 (W.D. Va. Feb. 12, 2014)	41
<i>Baptist Health v. Murphy</i> , 226 S.W.3d 800 (Ark. 2006)	59
<i>Beck v. McDonald</i> 848 F.3d 262 (4th Cir. 2017), <i>cert. denied sub nom. Beck v. Shulkin</i> , 137 S. Ct. 2307 (2017).....	20
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	9
<i>Bellsouth Telecomms., LLC v. Cobb Cty.</i> , 802 S.E.2d 686 (Ga. Ct. App. 2017), <i>reconsideration denied</i> (July 12, 2017), <i>cert. granted</i> (Apr. 16, 2018)	39
<i>Bishop v. Shorter Univ., Inc.</i> , No. 4:15-CV-00033-HLM (N.D. Ga. June 4, 2015), ECF No. 22	33
<i>Bonaparte v. Tax Ct.</i> , 104 U.S. 592 (1881).....	54
<i>Bradley Ctr., Inc. v. Wessner</i> , 296 S.E.2d 693 (Ga. 1982)	25, 26
<i>Byrd v. English</i> 43 S.E. 419 (Ga. 1903)	36
<i>Campbell v. Albers</i> , 39 N.E.2d 672 (Ill. Ct. App 1942)	54
<i>Campbell v. Beak</i> , 568 S.E.2d 801 (Ga. Ct. App. 2002).....	68
<i>City of Waukesha v. E.P.A.</i> , 320 F.3d 228 (D.C. Cir. 2003).....	15
<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	16, 17, 21

<i>Collins v. Athens Orthopedic Clinic</i> , 815 S.E.2d 639 (Ga. Ct. App. 2018).....	36, 37
<i>Comm. Bank of Trenton v. Schnuck Markets, Inc.</i> , 887 F.3d 803 (7th Cir. 2018)	66, 67
<i>Common Cause/Georgia v. Billups</i> , 554 F.3d 1340 (11th Cir. 2009)	23
<i>Construction Lender, Inc. v. Sutter</i> , 491 S.E.2d 853 (Ga. Ct. App. 1997).....	37
<i>Consumer Financial Protection Bureau v. Frederick Hanna</i> , 114 F. Supp. 3d 1342, 1372-73 (N.D. Ga. 2015)	59
<i>Consumer Financial Protection Bureau v. RD Legal Funding, LLC</i> , No. 17-CV-890 (LAP), 2018 WL 3094916 (S.D.N.Y. June 21, 2018)	55
<i>Corbitt v. Walgreen</i> , 7:14-cv-017, 2015 WL 1726011 (M.D. Ga. April 15, 2015)	29
<i>Crespo v. Coldwell Banker Mortg.</i> , 599 F. App'x 868 (11th Cir. 2014)	55
<i>Crouch v. Teledyne Cont'l Motors</i> , No. 10-00072-KD-N, 2011 WL 1539854 (S.D. Ala. Apr. 21, 2011)	54
<i>Cruz v. FXDirectDealer</i> , 720 F.3d 115 (2d Cir. 2013) (NY)	55
<i>Erbar v. Rare Hosp. Int'l, Inc.</i> , 316 P.3d 937 (Okla. Ct. App. 2013)	59
<i>F.T.C. v. Lifelock Inc.</i> , No. 10-cv-00530, 2010 WL 1944122 (D. Ariz. Mar. 9, 2010)	42
<i>F.T.C. v. Wyndham Worldwide Corp.</i> , 799 F.3d 236 (3d Cir. 2015)	40, 57

<i>First Choice Federal Credit Union v. Wendy’s Co.</i> , No. 16-506, 2017 WL 9487086 (W.D. Pa. Feb. 13, 2017)	41, 58, 69
<i>Fla. Ass’n of Med. Equip. Dealers, Med-Health Care v. Apfel</i> , 194 F.3d 1227 (11th Cir. 1999)	22
<i>Flatirons Bank v. Alan W. Steinberg Ltd. P’ship</i> , 233 So.3d 1207 (Fla. Dist. Ct. App. 2017)	54
<i>Havens Realty Corp. v. Coleman</i> , 455 U.S. 363 (1982)	23
<i>Healey v. Beer Ins.</i> , 491 U.S. 324 (1989)	54
<i>Hendon Properties, LLC v. Cinema Dev.</i> , LLC, 620 S.E.2d 644 (Ga. Ct. App. 2005)	52
<i>Hershenow v. Enterprise Rent-A-Car Co. of Boston, Inc.</i> , 840 N.E.2d 526 (Mass. 2006)	65
<i>Higgins v. Bank of Am., N.A.</i> , No. 1:15-CV-01119, 2015 WL 12086083 (N.D. Ga. Sept. 22, 2015)	47, 48, 62
<i>Hill v. Morehouse Med. Assocs., Inc.</i> , No. 02-14429, 2003 WL 22019936 (11th Cir. Aug. 15, 2003)	60
<i>Hunt v. Wa. State Apple Advert. Comm’n</i> , 432 U.S. 333 (1977)	23
<i>In the Matter of Credit Karma, Inc.</i> , No. 132-3091, 2014 WL 4252397 (FTC Aug. 13, 2014)	42
<i>In the Matter of LabMD, Inc.</i> , No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016), <i>reversed on other grounds</i> , <i>LabMD, Inc. v. F.T.C.</i> , 894 F.3d 1221 (11th Cir. 2018)	40
<i>In the Matter of Paypal, Inc.</i> , No. 162-3102, 2018 WL 1182195 (F.T.C. Feb. 27, 2018)	43

<i>In the Matter of Paypal, Inc.,</i> No. 162-3102, 2018 WL 3046375 (F.T.C. May 23, 2018)	44
<i>In the Matter of Taxslayer, LLC,</i> No. 162-3063, 2017 WL 5477618 (F.T.C. Oct. 20, 2017)	43
<i>In the Matter of Taxslayer, LLC,</i> No. 162-3063, 2017 WL 5477619 (F.T.C. Oct. 20, 2017)	43
<i>In re Adobe Sys., Inc. Privacy Litig.,</i> 66 F. Supp. 3d 1197 (N.D. Cal. 2014)	16
<i>In re Arby's Rest. Grp. Inc. Litig. (Arby's II),</i> 317 F. Supp. 3d 1222, 1227-28 (N.D. Ga. 2018)	57, 58
<i>In re Arby's Rest. Grp. Inc. Litig.,</i> No. 1:17-CV-0514-AT, 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018)	<i>passim</i>
<i>In re Bates,</i> No. 09-51279-NPO, 2010 WL 2203634 (Bankr. S.D. Miss. May 27, 2010)	45, 46
<i>In re Equifax, Inc., Customer Data Security Breach Litig.,</i> 289 F. Supp. 3d 1322 (J.P.M.L. 2017)	67
<i>In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.,</i> No. 1:14-MD-2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016)	<i>passim</i>
<i>In re Hydroxycut Mktg. & Sales Practices Litig.,</i> 299 F.R.D. 648 (S.D. Cal. 2014)	64
<i>In re Killian,</i> No. ADV. 08-80250-HB, 2009 WL 2927950 (Bankr. D.S.C. July 23, 2009)	47
<i>In re Managed Care Litig.,</i> 298 F. Supp. 2d 1259 (S.D. Fla. 2003)	24

<i>In re SuperValu, Inc</i> 870 F.3d 763 (8th Cir. 2017)	19, 22
<i>In re Target Corp. Customer Data Sec. Breach Litig.</i> , 64 F. Supp. 3d 1304 (D. Minn. 2014).....	66
<i>In re TJX Cos. Retail Sec. Breach Litig.</i> , 564 F.3d 489 (1st Cir. 2009).....	42, 57
<i>In re Zappos.com, Inc.</i> , 888 F.3d 1020 (9th Cir. 2018)	20
<i>ITCO Corp. v. Michelin Tire</i> , 722 F.2d 42 (4th Cir. 1983)	55
<i>Jenkins v. Wachovia Bank N.A.</i> , No. 09C57922, 2010 WL 10063830 (Ga. St. Ct., Gwinnett Cty. Sept. 21, 2010)	47
<i>Jenkins v. Wachovia Bank N.A.</i> , No. A11A2053, 2013 WL 6836900 (Ga. App. Ct. Aug. 20, 2013)	47
<i>Johannaber v. Emory Univ.</i> , No. 1:08-CV-2201-TWT, 2009 WL 10671453 (N.D. Ga. Dec. 14, 2009)	60
<i>Katz v. Pershing</i> , 806 F. Supp. 2d 452 (D. Mass. 2011).....	65
<i>Klairmont v. Gainsboro Rest., Inc.</i> , 987 N.E.2d 1247 (Mass. App. Ct. 2013)	65
<i>Krottner v. Starbucks Corp.</i> , 628 F.3d 1139 (9th Cir. 2010)	20
<i>Kull v. Six Flags Over Georgia II, L.P.</i> , 592 S.E.2d 143 (Ga. Ct. App. 2003).....	39
<i>LabMD, Inc. v. FTC</i> , 894 F.3d 1221 (11th Cir. 2018)	41, 42

<i>Laroche v. CSX Transport., Inc.</i> , No. CV 5 13-86, 2015 WL 5179011 (S.D. Ga. Sept. 3, 2015).....	47
<i>Lee St. Auto Sales, Inc. v. Warren</i> , 116 S.E.2d 243 (Ga. Ct. App. 1960).....	25
<i>Lee v. Rodriguez</i> , No. 3:06-CV-083-JTC, 2008 WL 11417307 (N.D. Ga. June 24, 2008)	40
<i>Legacy Acad., Inc. v. Mamilove, LLC</i> , 761 S.E.2d 880 (Ga. Ct. App. 2014), <i>vacated on other grounds</i> , 777 S.E.2d 731 (Ga. Ct. App. 2015).....	41
<i>Lisk v. Lumber One Wood Preserving, LLC</i> , 792 F.3d 1331 (11th Cir. 2015)	64
<i>Malak v. First Nat’l Bank of Atlanta</i> , 393 S.E.2d 267 (Ga. Ct. App. 1990).....	37
<i>McConnell v. Georgia Dep’t of Labor</i> , 814 S.E.2d 790 (Ga. Ct. App. 2018), <i>cert. pending</i> , Nos. S18C1316 and S18C1317 (Ga. May 31, 2018).....	4, 25, 27, 64
<i>McConnell v. Georgia Dep’t of Labor</i> , 337 Ga. App. 457 (2016)	28
<i>McLain v. Mariner Health Care, Inc.</i> , 631 S.E.2d 435 (Ga. Ct. App. 2006).....	38, 39
<i>MedImmune, Inc. v. Genentech, Inc.</i> , 549 U.S. 118 (2007).....	68
<i>Miles Rich Chrysler-Plymouth, Inc. v. Mass.</i> , 411 S.E.2d 901 (Ga. Ct. App. 1991).....	61
<i>Mounce v. CHSPSC, LLC</i> , No. 5:15-CV-05197, 2017 WL 4392048 (W.D. Ark. Sept. 29, 2017)	64

<i>New York State Bar Ass’n v. FTC</i> , 276 F. Supp. 2d 110 (D.D.C. 2003).....	45
<i>Nicholas Homes, Inc. v. M & I Marshall & Ilsley Bank, N.A.</i> , No. CV09-2079-PHX-JAT, 2010 WL 1759453 (D. Ariz. Apr. 30, 2010)	46
<i>Owens v. Dixie Motor Co.</i> , No. 5:12-CV-389-FL, 2014 WL 12703392 (E.D.N.C. Mar. 31, 2014)	46
<i>Pedro v. Equifax, Inc.</i> , 868 F.3d 1275 (11th Cir. 2017)	13
<i>Pisciotta v. Old Nat. Bancorp.</i> , 499 F.3d 629 (7th Cir. 2007)	17, 18
<i>Powell v. McCormack</i> , 395 U.S. 486 (1969).....	68
<i>Raleigh & G.R. Co. v. Lowe</i> , 28 S.E. 867 (Ga. 1897)	30, 38
<i>Ray v. Spirit Airlines, Inc.</i> , 767 F.3d 1220 (11th Cir. 2014)	9
<i>Reilly v. Ceridian Corp.</i> 664 F.3d 38 (3d Cir. 2011)	20
<i>Resnick v. AvMed, Inc.</i> , 693 F.3d 1317 (11th Cir. 2012)	<i>passim</i>
<i>Robert & Co. Assocs. v. Rhodes-Haverty P’ship</i> , 300 S.E.2d 503 (Ga. 1983)	47, 48
<i>Rogers v. Omni Sol.</i> , No. 10-21588-CIV, 2010 WL 4136145 (S.D. Fla. Oct. 19, 2010).....	55
<i>Ruk v. Crown Asset Mgmt., LLC</i> , No. 1:16-CV-03444-LMM, 2017 WL 3085686 (N.D. Ga. June 8, 2017)	61

<i>Saladin v. City of Milledgeville</i> , 812 F.2d 687 (11th Cir. 1987)	13
<i>Sawyer v. Market Am. Inc.</i> , 661 S.E.2d 750 (N.C. Ct. App. 2008).....	54
<i>Schernekau v. McNabb</i> , 470 S.E.2d 296 (Ga. Ct. App. 1996).....	33
<i>State Farm Mut. Ins. Co. v. Campbell</i> , 538 U.S. 408 (2003).....	54
<i>Stelts v. Epperson</i> , 411 S.E.2d 281 (Ga. Ct. App. 1991).....	34
<i>Summers v. Earth Island Inst.</i> , 555 U.S. 488 (2009).....	24
<i>Sun Trust Banks, Inc. v. Killebrew</i> , 464 S.E.2d 207 (Ga. 1995)	31, 32
<i>Susan B. Anthony List v. Driehaus</i> , 134 S. Ct. 2334 (2014).....	17
<i>Teague v. Keith</i> , 108 S.E.2d 489 (Ga. 1959)	38
<i>Town of Chester, N.Y. v. Laroe Estates, Inc.</i> , 137 S. Ct. 1645 (2017).....	10
<i>U.S. v. Students Challenging Regulatory Agency Procedures</i> (<i>SCRAP</i>), 412 U.S. 669 (1973).....	11
<i>United States v. Whatley</i> , 719 F.3d 1206 (11th Cir. 2013)	18
<i>Van Tassell v. United Mktg. Grp.</i> , 795 F. Supp. 2d 770 (N.D. Ill. 2011) (IL)	55

<i>Warner v. Arnold</i> , 210 S.E.2d 350 (Ga. Ct. App. 1974).....	30, 33
<i>Wells Fargo Bank, N.A. v. Jenkins</i> , 744 S.E.2d 686 (Ga. 2013)	43, 46, 47
<i>Wells v. Willow Lake Estates, Inc.</i> , 390 F. App'x 956 (11th Cir. 2010)	15

Statutes, Rules and Regulations

United States Code	
15 U.S.C. §6801(a)	14, 15, 16
28 U.S.C. §2201	68, 69
Code of Federal Regulations	
12 C.F.R. Parts 30 (App. B), 208 (App. D-2), 225 (App. F), 364 (App. B), 570 (App. B)	14
16 C.F.R. Part 314	<i>passim</i>
16 C.F.R. §314.1(b)	14, 44, 45, 46
16 C.F.R. §314.4(c)	44
16 C.F.R. §314.4(e)	14, 44
16 C.F.R. §681.1(d)(1).....	14
Federal Rules of Civil Procedure	
Fed. R. Civ. P. 8	13, 48
Fed. R. Civ. P. 9(b)	48, 59, 60
Fed. R. Civ. P. 23	64

State Statutes

Fla. Stat. §501.204(1)	59
Minn. Stat. §325D.45.....	62
Minn. Stat. §325E.64	66
N.M. Stat. Ann. §57-12-2	59

O.C.G.A. §10-1-399	68
O.C.G.A. §13-6-11	68
N.R.S.A. §87-303(b).....	62
Mass. Gen. Laws Ch. 93A	65
Mass. Gen. Laws Ch. 93H.....	65

Other Authorities

Ga. Ct. App. R. 33.2(a)(1)	36
RESTATEMENT OF TORTS §766C (1979).....	36
RESTATEMENT (SECOND) OF TORTS §282.....	26
RESTATEMENT (SECOND) OF TORTS, §302B (1965)	29, 32
RESTATEMENT (SECOND) OF TORTS, §552 (1977).....	48
Wright and Miller, FEDERAL PRACTICE AND PROCEDURE, §3531.4 n.7	13

Financial Institution Plaintiffs and Association Plaintiffs (collectively, “Plaintiffs”)¹ submit this memorandum of law in opposition to Defendants Equifax Inc.’s and Equifax Information Services LLC’s (“Equifax”) Motion to Dismiss (“Motion”) (ECF No. 435) Plaintiffs’ Consolidated Amended Complaint (“Complaint”) (ECF No. 390).

INTRODUCTION

The Equifax data breach compromised the nation’s entire credit reporting and verification system, which Equifax refers to as the “Modern Credit Landscape.” Plaintiffs and the Class of financial institutions, as providers and purchasers of information within this landscape, are the most direct and foreseeable victims of Equifax’s conscience-shocking data breach, in which approximately 147 million U.S. consumers – roughly 46% of the U.S. population and nearly 60% of all adults in the U.S. – had their highly sensitive, personally-identifying information (“PII”) and payment card data (“PCD”) compromised between May and July 2017 (the “Data Breach”). As Plaintiffs allege, the Data Breach was the direct result of Equifax’s active mismanagement of its data security measures.

Equifax could have prevented the Data Breach by implementing the most basic and necessary precautions to safeguard PII and PCD. But time and time

¹ For ease of reference, the brief will refer to “Plaintiffs;” however, Association Plaintiffs only join in Count 25 for declaratory and equitable relief.

again, Equifax ignored explicit warnings. In the months preceding the Data Breach, Equifax suffered no fewer than *five* data breaches that compromised PII. When hackers took advantage of a publicly known vulnerability that Equifax specifically had been warned about, Equifax's woefully deficient data security measures failed to detect the intrusion, and the hackers were able to spend two months roaming Equifax's systems unfettered, exfiltrating hundreds of millions of lines of consumer data. As a result, the PII and PCD, which flows within the nation's credit reporting and verification system and is essential for its secure operation was compromised and is now in the hands of identity thieves. Financial institutions can no longer rely upon the personally identifying characteristics of their customers' PII because this information, which was once unique and protected, is now ubiquitous. In short, Equifax has destroyed the consumer credit ecosystem. The resulting harm to Plaintiffs and the Class, which are direct participants in the nation's credit reporting and verification system, could not be more foreseeable.

Contrary to Equifax's arguments, it is not Plaintiffs' theory of liability that is unprecedented; rather, it is the scope and impact of the Equifax Data Breach, which is arguably the most damaging data breach in the nation's history. Although Plaintiffs plausibly allege that Equifax had a duty to act reasonably in managing

the security of the PII and PCD with which it was entrusted, Equifax argues it owed no duty to Plaintiffs to act reasonably to protect such information despite its repeated public representations to the contrary. Equifax further claims that Plaintiffs have failed to plead any plausible injury and instead *voluntarily* incurred out-of-pocket costs. Equifax does so by ignoring or misconstruing the factual allegations, which clearly allege that Plaintiffs have suffered, and continue to suffer, losses directly associated with Equifax's actions. Setting aside Equifax's hyperbole, Plaintiffs' theory is neither "far-fetched" nor unprecedented. Plaintiffs' theory of liability is simple and straight-forward: Equifax had a general duty to act reasonably in its conduct to avoid foreseeable harm to foreseeable parties. Separately, Equifax affirmatively acknowledged and undertook the duty to act reasonably to protect PII and PCD, fully aware of the harm that would result to Plaintiffs and the Class if it failed to do so.

As discussed below, Plaintiffs have plausibly pleaded claims of negligence, negligence per se, negligent misrepresentation, and violation of various state statutes and for appropriate equitable relief. In similar cases seeking to recover losses from defendants that, like Equifax, maintained inadequate data security, this Court, and another in this District, have rejected the arguments Equifax now raises. *See In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-

2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016); *In re Arby's Rest. Grp. Inc. Litig.* (“*Arby's I*”), No. 1:17-CV-0514-AT, 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018). Equifax’s primary rejoinder to this authority is to repeatedly cite *McConnell v. Georgia Dep’t of Labor*, 814 S.E.2d 790 (Ga. Ct. App. 2018), *cert. pending*, Nos. S18C1316 and S18C1317 (Ga. May 31, 2018) (“*McConnell III*”). *McConnell III*, however, does not negate Georgia’s common law duty of reasonable care to avoid causing foreseeable injury to others, *Home Depot*, 2016 WL 2897520, at *4; *Arby's I*, 2018 WL 2128441, at *3-7, nor does it have any relevance to the other claims that Plaintiffs have plausibly pleaded. Thus, Equifax’s Motion should be denied.

FACTUAL BACKGROUND

Equifax’s motto is “*Powering the World with Knowledge.*” In short, Equifax’s business is information. Operating as a consumer reporting agency (“CRA”), Equifax accumulated sensitive consumer data and related consumer information on over 800 million individuals. ¶¶1, 104, 125.² This information includes PII, such as names, Social Security numbers, birth dates, addresses, and driver’s license numbers. ¶¶100-101.

Plaintiffs are financial institutions that provide a range of financial services

² Citations to “¶ __” refer to the Complaint.

to consumers, including deposit accounts, payment cards, lending, and other credit-related facilities. The credit reporting and verification system functions because of the symbiotic relationship between Plaintiffs and Equifax. ¶¶97-99. Financial institutions gather and submit to Equifax information about their customers, including their payment histories. ¶100. Equifax compiles this information into credit reports and other products, which financial institutions then rely on to verify the identity of individuals, make credit determinations, and extend credit and credit-related services to consumers. ¶97. The PII and related information that financial institutions provide to Equifax and that Equifax utilizes for its reports and other products is extremely valuable for its accuracy and authenticity, enabling Plaintiffs to identify and determine the credit-worthiness of individuals. The credit reporting and verification system worked because the information within the system was unique and secure.

Equifax serves as the “linchpin” of the nation’s credit reporting and verification system and acknowledges that the collection of consumer information and data carries with it an enormous responsibility to protect that data from exposure to unauthorized third parties. ¶¶1, 97. Indeed, Equifax represents itself as a “trusted steward” of PII, given its role in the system. For example, it states:

Equifax is a trusted steward of credit information for

thousands of financial institutions and businesses, and millions of consumers. *We take this responsibility seriously, and follow a strict commitment to data excellence that helps lenders get the quality information they need to make better business decisions.* ¶125.

Equifax further represents that “*securing data is the core value of our company,*” acknowledging the extraordinary importance of securing the PII it receives and the special relationship that exists between Equifax and financial institutions within the credit reporting and verification system.³

The Equifax Data Breach is the direct result of Equifax’s affirmative misconduct and refusal to take the steps necessary to properly protect PII consistent with its representations. The Data Breach is not an isolated incident, but is part of Equifax’s long history of taking insufficient and inadequate data security measures. In the months leading up to the Data Breach, Equifax’s deficient data security measures led to multiple security breaches that compromised consumer PII. ¶¶150-58. Similarly, numerous research analysts and security experts specifically warned Equifax that its security measures were deficient and left the company “vulnerable to data theft and security breaches.” ¶¶158-64. Despite these warnings, Equifax continued to actively mishandle its data security and did not take steps to correct known vulnerabilities to its systems or otherwise ensure

³ Richard Smith, Former Chief Executive Officer of Equifax Inc., Nov. 8, 2017 Hearing, U.S. Senate Committee on Commerce, Science & Transportation.

that the PII and PCD it maintained was secure.

On September 7, 2017, Equifax announced that between May 13 and July 30, 2017, hackers exploited a known vulnerability in Equifax’s U.S. web server software to gain access to and steal the PII of approximately 147 million U.S. consumers – roughly 46% of the U.S. population and nearly 60% of all adults in U.S. – at least one family member in every household. ¶¶3, 166. The Equifax Data Breach is arguably the most damaging data breach in the nation’s history and was the direct result of Equifax’s actions, which left critical systems vulnerable to attack. ¶¶3-5. Specifically, Equifax failed to patch known vulnerabilities in Apache Struts, an open-source application framework that supports Equifax’s online dispute portal web application. ¶167.

In March 7, 2017, the Apache Struts vulnerability was discovered and several entities, including The Apache Foundation, the U.S. Department of Commerce’s National Institute of Standards and Technology (“NIST”), and the U.S. Department of Homeland Security’s Computer Emergency Readiness Team (“U.S. CERT”), immediately issued public warnings regarding the vulnerability. ¶176. On that same day, The Apache Foundation also made available various patches and workarounds that eliminated the vulnerability. ¶177.

Equifax acknowledges that its security team “was aware of this vulnerability

[with Apache Struts] at that time [in March 2017]” and that the patches provided by The Apache Foundation would have eliminated the vulnerability. ¶179. Although Equifax ran security scans on March 15, 2017 that could have alerted Equifax to the Apache Struts vulnerability, Equifax’s practice of not maintaining proper security certificates prevented it from detecting the Apache Struts vulnerability and directly led to the hackers’ ability to exploit the vulnerability and gain access to Equifax’s servers. ¶¶181-82. Equifax did not discover the Data Breach until July 29, 2017, over four and a half months after the Apache Struts vulnerability was announced. ¶196. Compounding Plaintiffs’ injuries, Equifax failed to publicly disclose the breach for another thirty days. ¶¶196-203.

Following the disclosure of the Data Breach, former Equifax employees who worked on or alongside the Equifax security team confirmed that Equifax did not place a high priority on data security. ¶215. When asked about Equifax’s attitude towards data security, a former employee stated: “[g]iven the amount of data they have access to and the sensitivity to us, security isn’t at the forefront of everybody’s mind, not how it should be.” *Id.*

Equifax’s actions directly undermined the credit reporting and verification system by exposing the PII that is used to identify consumers whose credit information is reported and analyzed within the system. ¶¶105-06. This massive

exposure of consumer PII has directly injured Plaintiffs and the Class because they can no longer rely on such information for purposes of identifying their customers.

¶247. Consequently, contrary to Equifax’s arguments, Plaintiffs have incurred direct out-of-pocket costs to respond to the compromise of the credit reporting and verification system Plaintiffs use to verify their customers’ identities, to identify and monitor fraudulent banking activities, to respond to customers’ concerns and complaints regarding the Equifax Data Breach, and to cancel and reissue compromised payment cards. ¶¶12-57, 247-48, 251, 252.

ARGUMENT AND CITATION OF AUTHORITY

A complaint should be dismissed only where the facts alleged fail to state a “plausible” claim for relief. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Factual allegations must be taken as true and construed in the light most favorable to the plaintiff. *Ray v. Spirit Airlines, Inc.*, 767 F.3d 1220, 1223 (11th Cir. 2014). Generally, notice pleading is all that is required. *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012). The complaint need only provide fair notice of the claim and the grounds upon which it rests. *See Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007). The Complaint meets this pleading standard.

I. Plaintiffs Have Article III Standing

A. Plaintiffs Suffered Injuries-in-Fact Traceable to the Equifax Data Breach

To establish Article III standing, a plaintiff must have ““(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.”” *Town of Chester, N.Y. v. Laroe Estates, Inc.*, 137 S. Ct. 1645, 1650 (2017).⁴ Equifax raises only two arguments: (1) that Plaintiffs’ actions in response to the Data Breach constituted a merely speculative or self-inflicted injury; and (2) to the extent Plaintiffs suffered an injury, it is traceable not to the *Equifax* Data Breach, but to *every other* data breach. Both arguments ignore the well-pleaded allegations and should be rejected.

1. Plaintiffs Suffered Injuries-in-Fact

Plaintiffs have already suffered four distinct injuries in fact as a direct result of the Data Breach, any one of which is sufficient to confer Article III standing: (1) Plaintiffs have *already* spent time and money responding to the compromise of the credit reporting system and the PII that Plaintiffs rely on to verify their customers’ identities; (2) Plaintiffs have *already* spent time and money assessing the impact of the Data Breach as required by federal law; (3) Plaintiffs that issued payment cards

⁴ Unless otherwise indicated, citations are omitted and emphasis is added.

compromised in the Data Breach have *already* spent time and money canceling and reissuing affected payment cards and/or reimbursing customers for fraudulent transactions; and (4) each Plaintiff has *already* spent time and money to mitigate what experts universally acknowledge is a substantial risk of future fraudulent banking activity.⁵

a. The Compromise of the Credit Reporting and Verification System Constitutes an Injury to All Plaintiffs.

Equifax claims that Plaintiffs’ allegations regarding the time and money spent addressing harms is conjectural. Unlike other data breaches that compromised PCD alone, however, the Data Breach additionally compromised the PII that forms the backbone of the credit reporting and verification system that Plaintiffs actively rely on to verify customers’ identities and make credit determinations. ¶¶12-57 (“*In order to provide financial services to consumers*, [each Plaintiff] relies on the accuracy and integrity of the information supplied by the credit reporting system.”); ¶105 (Plaintiffs “rely on the very PII elements that were exposed in the Equifax Data Breach . . . to verify the identity of their

⁵ Equifax chides Plaintiffs for making uniform allegations of harm, failing to recognize that its negligence harmed Plaintiffs and the Class in uniform ways. ¶¶234-35, 244; *U.S. v. Students Challenging Regulatory Agency Procedures (SCRAP)*, 412 U.S. 669, 687 (1973) (“[S]tanding is not to be denied simply because many people suffer the same injury.”).

customers for all the financial services they offer.”). Thus, the Complaint alleges that the compromise of that verification system has already harmed each Plaintiff. *See, e.g.*, ¶¶7-10, 105-06, 236; ¶241 (“[T]he foundation that banks and credit unions use to control new account fraud or application fraud is badly damaged.”); ¶246 (SSNs “should not be used to validate anyone’s identity, ever again.”); ¶249 (“Banks and fintechs will need to closely evaluate their processes in light of the Equifax breach to make sure the information they are getting is still accurately verifying their online customers.”).

The direct out of pocket costs resulting from the Data Breach are not “voluntarily” chosen as Plaintiffs are ***required*** to protect their customers’ accounts. *See supra* Section I.A.1.b; ¶¶116-23. These costs include the monies Plaintiffs spent resulting from the harm to the credit reporting and verification system and include the cost of implementing additional measures to safeguard “their authentication policies, protocols, procedures, and measures” for verifying the identities of their customers. ¶¶12-57 & 244. Plaintiffs have also expended time and money fielding calls from “customers regarding their concerns about identity theft and the safety of their accounts” in light of the Data Breach.⁶ ¶¶12-57. Such

⁶ Equifax disputes the allegations that customers called their banks in the wake of the most consequential data breach in history and demands that Plaintiffs plead such allegations with particularity. Br. at 22 n.7. A short and plain

injuries are far from conjectural. *Resnick*, 693 F.3d at 1323 (incurring monetary damages in the wake of a data breach “constitutes an injury in fact under the law”); Wright and Miller, FEDERAL PRACTICE AND PROCEDURE, §3531.4 n.7; *Pedro v. Equifax, Inc.*, 868 F.3d 1275, 1280 (11th Cir. 2017) (time spent responding to unlawful acts constitutes concrete injury).⁷ Indeed, the Complaint alleges these injuries continue. ¶¶12-57. Every time a Plaintiff needs to verify the identity of a customer, because the underlying information has been compromised due to Equifax’s actions, the Data Breach injures them anew. *Id.*

b. Federal Law Required All Plaintiffs to Take Action in Response to the Data Breach.

Equifax claims that faced with the most consequential data breach in history, Plaintiffs were not “required . . . to investigate the data breach,” speculating that Plaintiffs did so only for “commercial reasons.” Br. at 16.⁸ Federal law, however, obligated Plaintiffs to investigate the Data Breach and the time and money spent on such investigations constitutes injury in fact.

statement, ¶¶12-57, is all that is required. Fed. R. Civ. P. 8.(a)(2).

⁷ Because all Plaintiffs suffered these injuries, Plaintiffs need not establish that any other injury also satisfies Article III. *Saladin v. City of Milledgeville*, 812 F.2d 687, 690 n.3 (11th Cir. 1987) (finding of standing as to one injury “makes it unnecessary” to consider other injuries).

⁸ References to “Br.” are to Defendants’ Memorandum in Support of Defendants’ Motion to Dismiss the Financial Institutions’ Consolidated Amended Complaint, ECF No. 435-1.

The Gramm-Leach-Bliley Act (“GLBA”) applies to “each financial institution,” including Plaintiffs, and confers “an affirmative and continuing obligation” to protect the security of customers’ PII. 15 U.S.C. §6801(a). Rules promulgated pursuant to the GLBA require Plaintiffs not just to develop, implement, and maintain an information security program to “[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information,” 16 C.F.R. §314.4(b), but to “evaluate and adjust” that program “in light of . . . any other circumstances that [they] know or have reason to know may have a material impact on [their] information security program.” *Id.* §314.4(e); *see also* Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. Parts 30 (App. B), 208 (App. D-2), 225 (App. F), 364 (App. B), 570 (App. B), & 748 (App. A).

Similarly, the Fair Credit Reporting Act (“FCRA”) requires Plaintiffs to implement an identity theft prevention program to “detect, prevent, and mitigate identity theft.” 16 C.F.R. §681.1(d)(1). Plaintiffs must “ensure” that their programs are updated “to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.” *Id.* §681.1(d)(2)(iv).

The Data Breach compromised the confidentiality, and integrity of

Plaintiffs’ customers’ PII and PCD and placed Plaintiffs and their customers at greater risk of identity theft and related financial fraud. *See, e.g.*, ¶¶8-10, 105-06, 236, 241, 246, & 249.⁹ Plaintiffs were thus obligated to investigate the impact of the Data Breach. As the Eleventh Circuit has held, spending “time and money complying with regulations” constitutes an injury in fact for purposes of Article III standing. *Wells v. Willow Lake Estates, Inc.*, 390 F. App’x 956, 959 (11th Cir. 2010); *see also City of Waukesha v. E.P.A.*, 320 F.3d 228, 234 (D.C. Cir. 2003).

Equifax’s attempt to characterize Plaintiffs’ actions as “voluntary” ignores reality and conflicts with the “affirmative and continuing obligation” Congress has imposed on Plaintiffs (and Equifax) to respond to known threats to customers’ PII. 15 U.S.C. §6801(a). The resulting regulatory scheme is designed to remove discretion from financial institutions that might argue, as Equifax does, that inaction in the face of such threats represents a plausible course of action.

c. FI Card Plaintiffs Have Suffered Additional Injuries

FI Card Plaintiffs “issued payment cards that were compromised in the Data Breach and received fraud alerts from one or more of the payment card brands identifying payment cards it issued that were compromised.” ¶¶13, 14, 17, 20, 23,

⁹ Equifax suggests Plaintiffs claim injury on the basis of “the increased risk of future identity theft to their customers.” Br. at 19. Plaintiffs allege injuries stemming only from the harm they have and will suffer as a result of the Data Breach. ¶237.

25, 31-33, 36, 39, 44, 46, 47-52, 54-56, & 252. As a result, each FI Card Plaintiff incurred “direct out of pocket costs to protect . . . affected payment card accounts.” *Id.* These include the costs FI Card Plaintiffs incurred to cancel and reissue payment cards with new payment card data. *Id.*; ¶252. Equifax claims, without support, that when confronted with the theft of “only” 209,000 credit card numbers,¹⁰ it was not “justifiable” for FI Card Plaintiffs to cancel and reissue the affected cards. Br. at 21. To allege that the exposure of nearly a quarter million credit card numbers created a substantial risk of harm to the issuing financial institutions is not just plausible – it is obvious¹¹ – and FI Card Plaintiffs “reasonably incur[red] costs to mitigate or avoid that harm,” that are sufficient to confer Article III standing.¹² *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 414 n.5

¹⁰ Equifax argues that “the FI Plaintiffs do not even specify plausible facts regarding whether they issued those compromised cards.” Br. at 21. Notwithstanding Equifax’s failure to explain how FI Card Plaintiffs could cancel or reissue cards they did not issue, each FI Card Plaintiff specifically alleged that it “received fraud alerts from one or more of the payment card brands identifying payment cards *it issued* that were compromised.” ¶¶13, 14, 17, 20, 23, 25, 31-33, 36, 39, 44, 46, 47-52, 54-56.

¹¹ Even Equifax warns as much. *See, e.g.*, ¶¶133-34 & 239.

¹² Courts do not require plaintiffs to trade the implementation of reasonable mitigation measures for Article III standing. Indeed, “requiring Plaintiffs to wait for the threatened harm to materialize in order to sue would pose a standing problem of its own, because the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not ‘fairly traceable’ to the defendant’s data breach.” *In re Adobe*

(2013); *Home Depot*, 2016 WL 2897520, at *3 (the “costs to cancel and reissue cards compromised in the data breach . . . are not speculative and are not threatened future injuries, but are actual, current, monetary damages”).

d. The Most Consequential Data Breach in History Has Exposed All Plaintiffs to a Substantial Risk of Fraudulent Banking Activity

To have Article III standing “[a]n allegation of future injury may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.” *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014); *Clapper*, 568 U.S. at 414 n.5. Although not addressed by the Eleventh Circuit, *see Resnick*, 693 F.3d at 1323, in the context of a data breach where hackers target and compromise sensitive PII and PCD, courts have not hesitated to hold that “the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant’s actions.” *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 634 & nn.2-4 (7th Cir. 2007) (collecting cases).

Plaintiffs face a substantial and impending risk of future harm in the form of future fraudulent banking activity as a direct result of the Data Breach. ¶¶7-10, 12-

Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014).

57, 105-06, 234-60. As alleged, the primary harm caused by identity theft is not suffered by the individual whose identity is stolen; rather, the primary harm is suffered by the financial institutions that bear the risk of loss when identity thieves use a customer's PII to open accounts, transfer funds, take out loans, make fraudulent transactions, or obtain credit or debit cards in the customer's name. ¶¶237–39. Equifax itself detailed the injuries stemming from identity theft. ¶239. These are crimes directed against financial institutions designed to obtain money from them; an individual's PII is the key (obtained through Equifax's negligence) that the criminal uses to unlock the financial institutions' doors. It is widely recognized that Plaintiffs and the Class face a substantial risk of harm from the theft of PII and the resulting monies stolen. ¶¶7-10, 12-57, 106, 218, 234-40, 245.

Equifax does not dispute that Plaintiffs incurred costs to mitigate the harm of fraudulent banking activity, but instead speculates that the risk of harm that Plaintiffs face is insubstantial because hackers *might not* leverage the PII and PCD stolen in the most consequential data breach in history to commit fraud. Common sense says otherwise.¹³ *Id.*; ¶245 (“If names and Social Security numbers and

¹³ Equifax muses that, perhaps, the stolen data might not be used to commit fraud. But “[h]ackers easily can sell such stolen data.” ¶138. Why steal data if not to use it? Equifax is silent on this point, and indeed, offers nothing to suggest that it is implausible to accept that criminals seek to profit from the compromised PII. *See, e.g., United States v. Whatley*, 719 F.3d 1206, 1208 (11th Cir. 2013)

dates of birth are out there, they will be used at some point.”); ¶247 (“[A]ll of this data is being bought and sold.”); *see also* *Bailey v. Wheeler*, 843 F.3d 473, 482 (11th Cir. 2016). Not only is this argument inappropriate on a motion to dismiss, but the authority Equifax cites shows that Plaintiffs’ allegations are sufficient to confer Article III standing. For example, the Eighth Circuit in *In re SuperValu, Inc.*, held that consumers did not face a substantial risk of new account fraud – “the type of identity theft generally considered to have a more harmful direct effect” – because the data stolen there did “not include any personally identifying information, such as social security numbers, birth dates, or driver’s license numbers.” 870 F.3d 763, 770 (8th Cir. 2017). Here, “the foundation that [Plaintiffs] use to control new account fraud . . . is badly damaged,” ¶241, because the Data Breach compromised “sensitive personal information, including names, Social Security numbers, birth dates, addresses, and driver’s license numbers.” ¶184; *see also* ¶3.

In *Beck v. McDonald*, the Fourth Circuit found that a “misplaced” laptop did not present a substantial risk of future identity theft in part because there was no suggestion that “the data thief intentionally targeted the personal information

(“When asked why he robbed banks, legend has it that famed American bank robber Willie Sutton replied, ‘Because that’s where the money is.’”).

compromised.” 848 F.3d 262, 274 (4th Cir. 2017), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307 (2017). But here, Equifax itself acknowledged: “We are **regularly the target** of attempted cyber and other security threats.” ¶133; *see also* ¶¶133-34, 138, 149, & 284. Equifax even explained that hackers target the data compromised: the “personally identifiable information of our customers, employees, consumers and suppliers.” ¶133.

In *Reilly v. Ceridian Corp.*, the Third Circuit found that the plaintiff’s allegations of substantial risk were implausible in part because “no identifiable taking occurred.” 664 F.3d 38, 44 (3d Cir. 2011). Here, in a “statement for the record,” Equifax concedes that a taking occurred – the names, dates of birth, addresses, social security numbers, and drivers’ licenses of approximately 147 million Americans. ¶¶186-195.

In its attempt to avoid *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010), Equifax claims that the decision turned on the fact that “at least one plaintiff alleged that the information had been used to open an account.” Br. at 22 n.5. But as the Ninth Circuit recently reaffirmed, it was “the sensitivity of the personal information, combined with its theft,” that led the Ninth Circuit to conclude that “plaintiffs had adequately alleged an injury in fact supporting standing.” *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018). Plaintiffs

at length plausibly allege that they have already faced an increased risk of fraudulent banking activity stemming from the compromise of their sensitive PII. ¶¶8-10, 12-57, 106, 218, 234-260. Accordingly, their efforts to mitigate those risks constitute injuries sufficient to confer Article III standing. *Clapper*, 568 U.S. at 414 n.5.

2. Plaintiffs' Injuries Are Traceable to the Equifax Data Breach

The Eleventh Circuit has found that in the context of a data breach, traceability is established where (1) a plaintiff made efforts to secure information; (2) defendant failed to secure that information; and (3) plaintiff's injury was incurred after the information was taken from defendant. *Resnick*, 693 F.3d at 1324. These elements are satisfied here.

Plaintiffs allege that both they and Equifax are obligated to secure the PII and PCD compromised in the Equifax Data Breach. ¶¶111-121 (“[I]nformation provided by financial institutions to CRAs must be protected at every level.”). Plaintiffs further allege that “the vast quantity of consumer data compromised as a result of the Data Breach is the same consumer data FI Plaintiffs use to conduct their business.” ¶234; ¶¶7, 9, 105. Because Equifax failed to secure that data, ¶¶150-195, Plaintiffs can no longer rely on the accuracy or authenticity of that data to determine the credit-worthiness and/or identity of their customers. *See, e.g.*,

¶¶8-10, 105, 236, 241, 246, & 249. Unlike the highly attenuated causal chain rejected in *Fla. Ass’n of Med. Equip. Dealers, Med-Health Care v. Apfel*, 194 F.3d 1227 (11th Cir. 1999), the time and money Plaintiffs spent responding to the Equifax Data Breach is thus squarely traceable to the Equifax Data Breach.¹⁴ *Resnick*, 693 F.3d at 1324.

Equifax’s authority does not suggest otherwise. Indeed, in *SuperValu, Inc.*, the court specifically declined to require plaintiffs to allege that a particular fraudulent charge occurred because of defendant’s data breach. 870 F.3d at 772. Rather, the Eighth Circuit held that traceability was satisfied where plaintiffs allege a connection between the deficiencies in defendant’s security systems and the theft of payment card information. *Id.* Plaintiffs have alleged in detail the connection between Equifax’s failure to patch the Apache Struts vulnerability and the theft of the consumer data Plaintiffs rely on to authenticate their customers. ¶¶166-195; ¶234. Plaintiffs have satisfied the traceability element of standing.

B. The Association Plaintiffs Have Article III Standing

The Association Plaintiffs have standing “based on both a diversion-of-resources theory and an associational standing theory.” *Arcia v. Fla. Sec’y of State*,

¹⁴ Equifax’s conjecture that Plaintiffs’ injuries are traceable not to the Equifax Data Breach, but to “other breaches,” Br. at 24-25, ignores Plaintiffs’ allegations and deserves no consideration at the pleading stage. *Bailey*, 843 F.3d at 482.

772 F.3d 1335, 1341 (11th Cir. 2014).

1. The Association Plaintiffs Allege Diversion of Resources

Under the diversion-of-resources theory, an organization has standing to sue when a defendant's illegal acts impair the organization's ability to engage in its own projects by forcing the organization to divert resources in response. *See Havens Realty Corp. v. Coleman*, 455 U.S. 363, 379 (1982). Although ignored by Equifax, which paints the Association Plaintiffs' injuries as purely derivative, each Association Plaintiff alleges that it was forced to "divert and expend their own resources to assist members that have been harmed and continue to be harmed by the Equifax data breach." ¶85. This diversion of resources constitutes an injury in fact conferring Article III standing. *See Arcia*, 772 F.3d at 1340-2; *Common Cause/Georgia v. Billups*, 554 F.3d 1340, 1350 (11th Cir. 2009).

2. The Association Plaintiffs' Equitable Claim Does Not Require Member Participation

An association also has standing to sue when "(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Hunt v. Wa. State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977). Equifax challenges the first and third *Hunt* prongs. Both are satisfied.

The Association Plaintiffs represent financial institutions throughout the nation, ¶¶60-84, and as discussed above, individual financial institutions have standing to sue in this action. *See supra* Section I.A; ¶¶234-35, 244. Equifax claims that the Association Plaintiffs should be required to identify their affected members. Br. at 26. But the “requirement of naming the affected members” has been “dispensed with” where, as here, “*all* the members of the organization are affected by the challenged activity.” *Summers v. Earth Island Inst.*, 555 U.S. 488, 499 (2009). Thus, the first *Hunt* prong is met.

The third *Hunt* prong also is met. Members’ participation is not required for the issues on which the Association Plaintiffs seek equitable relief – Equifax’s legal duties regarding data security, the adequacy of its current security practices, and whether additional data security measures are needed. These issues turn entirely on Equifax’s conduct, not that of the Association Plaintiffs’ members. *See In re Managed Care Litig.*, 298 F. Supp. 2d 1259, 1307-08 (S.D. Fla. 2003) (“[I]t is well-established that an association may seek equitable relief on behalf of its members without running afoul” of the member participation requirement). Thus, the Association Plaintiffs have standing to pursue their claim for equitable relief. *Home Depot*, 2016 WL 2897520, at *5.

II. Plaintiffs State a Claim for Negligence

To state a claim for negligence, Plaintiffs must allege: “([1]) A legal duty to conform to a standard of conduct raised by the law for the protection of others against unreasonable risks of harm; (2) a breach of this standard; (3) a legally attributable causal connection between the conduct and the resulting injury; and, (4) some loss or damage flowing to the plaintiff’s legally protected interest as a result of the alleged breach of the legal duty.” *Lee St. Auto Sales, Inc. v. Warren*, 116 S.E.2d 243, 245 (Ga. Ct. App. 1960). Plaintiffs have satisfied each element.

A. Equifax Had a Duty to Plaintiffs

1. Equifax Had a Duty Not to Subject Plaintiffs to an Unreasonable Risk of Harm

Georgia law recognizes “a ‘general duty one owes to all the world not to subject them to an unreasonable risk of harm.’” *Arby’s I*, 2018 WL 2128441, at *3 (quoting *Bradley Ctr., Inc. v. Wessner*, 296 S.E.2d 693, 695 (Ga. 1982)); *see also Home Depot*, 2016 WL 2897520, at *3. Plaintiffs seek to hold Equifax to this basic duty, and Equifax advances no convincing reason why it should be exempted from the same standard of care that is as long-established as the common law itself.

Equifax argues that there is no duty under Georgia law to affirmatively “protect” PII, relying heavily on *McConnell v. Georgia Department of Labor*, 814 S.E.2d 790 (Ga. Ct. App. 2018). Br. at 28–33. But unlike the plaintiff in

McConnell, Plaintiffs do not allege that Equifax breached a novel, affirmative duty to protect PII. Rather, like in *Bradley*, Plaintiffs here allege that Equifax breached the long-recognized common law duty to use reasonable care in one's conduct to avoid causing foreseeable injury to others. *See Bradley*, 296 S.E.2d at 695 (“negligence is conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm.”); *see also* RESTATEMENT, (SECOND) OF TORTS §282. Contrary to Equifax's arguments, *McConnell III* is distinguishable because it did not address this general duty of care, but rather only considered whether defendant had an affirmative duty to protect PII absent any facts demonstrating foreseeable risk of harm.¹⁵ Plaintiffs here allege that Equifax, in undertaking its business operations of collecting and processing consumers' PII, had a general duty to do so in a reasonable manner to avoid foreseeable harm to others. *McConnell III* is therefore irrelevant because it did not consider application of the general duty recognized by the Georgia Supreme Court to not subject a party to an unreasonable risk of harm.

Moreover, *McConnell III* is factually distinguishable as the allegedly

¹⁵ Although Equifax makes much of the dicta that such a duty “has no source in Georgia statutory law or caselaw,” (Br. at 31), *McConnell III* considered only two potential sources for such a duty: the Georgia Personal Identity Protection Act and the Georgia Fair Business Practices Act (“GFBPA”). At no point did the court consider whether the plaintiff alleged a breach of the duty asserted here – the general duty not to subject persons to an unreasonable risk of harm.

negligent disclosure occurred when a state employee accidentally emailed approximately 1,000 Georgians and attached a spreadsheet with the PII of 4,000 individuals. *McConnell*, 814 S.E.2d at 793. McConnell did not allege that the Georgia Department of Labor ever previously experienced a similar negligent disclosure or had any reason to suspect that the specific employee involved was careless with sensitive data. Unlike in *McConnell III*, Equifax held itself out as a “trusted steward” of consumer data and acknowledged that the collection of PII required it to protect such data. Plaintiffs allege Equifax actively and negligently mishandled consumers’ PII and did not act reasonably in light of the foreseeable risk that its conduct would result in a data breach that would compromise PII and foreseeably harm Plaintiffs. ¶¶6, 137-185, 189, 208-215, 219-233, 291, 299, 303. In other words, unlike in *McConnell III*, Equifax’s own conduct created a foreseeable risk of harm to foreseeable victims. Thus, *McConnell III* does not require the Court to deviate from its prior decision in *Home Depot*, as Georgia courts still recognize a general duty to not subject foreseeable parties to an unreasonable risk of harm. In analyzing an earlier opinion in the *McConnell* case (with the same holding in pertinent part), the *Arby’s* court identified this duty as a fundamental, outcome-altering difference between *McConnell*, *Home Depot*, and the case before it:

Home Depot found a duty to protect [PII] ... “in the context of allegations that the defendant failed to implement reasonable security measures to combat a substantial data security risk of which it had received multiple warnings dating back several years and even took affirmative steps to stop its employees from fixing known security deficiencies.” ... There were, however, no similar allegations of known security deficiencies in *McConnell*. Nor were there any allegations that the action of the agency employee in ‘inadvertently’ emailing the spreadsheet containing the information was foreseeable.

Arby’s I, 2018 WL 2128441, at *6 (quoting *McConnell v. Georgia Dep’t of Labor*, 337 Ga. App. 457, 459 n.4 (2016)).

The *Arby’s* and *Home Depot* courts correctly applied Georgia law, and *McConnell III* does not contradict them. While it is true that in Georgia (as in most states) there is generally no ***affirmative*** duty to protect others against criminal activity, that broad rule does not apply in this case. The duty at issue here is not a “new” or affirmative duty imposed on a bystander to offer protection to a stranger. Instead, the specific questions for this Court are whether Equifax’s ***own actions*** created a foreseeable risk of a data breach or whether Equifax had reason to anticipate the likelihood of a breach on its systems that would foreseeably harm Plaintiffs. Plaintiffs assert that the answer to both of these questions is yes, and have alleged facts which plausibly support such a conclusion. Therefore, the Court should conclude at this stage that Plaintiffs sufficiently alleged Equifax owed them a duty of care and deny Equifax’s Motion.

As the *Arby's* court recently explained, under Georgia law, the concept of foreseeability is critical in determining the existence of a legal duty:

Negligence consists of exposing someone to whom a duty of care is owed to a foreseeable, unreasonable probability of harm. Foresight requires the ability to anticipate a risk of harm from the conduct in some form. Negligence is predicated on what should be anticipated[.]

Arby's I, 2018 WL 2128441, at *4; *see also Corbitt v. Walgreen*, 7:14-cv-017, 2015 WL 1726011, at *3 n.4 (M.D. Ga. April 15, 2015) (“The concept of ‘foreseeability’ in Georgia law seems to play a role both in defining a legal duty and in determining whether proximate cause exists.”).

As the Restatement recognizes, under appropriate circumstances, courts should find a duty to avoid exposing others to the risk of criminal conduct:

An act or an omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person which is intended to cause harm, even though such conduct is criminal.

RESTATEMENT (SECOND) OF TORTS, §302B (1965). Georgia courts have applied this same principle:

So far as scope of duty (or, as some courts put it, the relation of proximate cause) is concerned, it should make no difference whether the intervening actor is negligent or intentional, or criminal. Even criminal conduct by others is often reasonably to be anticipated. Thus, if a person leaves a borrowed car on the streets of almost any city with the doors unlocked and key in the ignition, that person is negligent (at least toward the owner) because of the very likelihood of theft.

Warner v. Arnold, 210 S.E.2d 350, 352 (Ga. Ct. App. 1974). Thus, the general rule that an intervening criminal act insulates an originally negligent defendant from liability is “inapplicable if the defendant (original wrongdoer) had reasonable grounds for apprehending” the criminal act that ultimately caused the harm. *Id.*

The *Arby's* court identified numerous examples of Georgia courts applying this rule in the context of premises liability cases. *See Arby's I*, 2018 WL 2128441, at *4 (collecting cases). The analogy to premises liability is apt, but analogous cases abound in other settings as well, and Georgia courts have applied these foundational principles of negligence flexibly to a wide variety of factual scenarios, including claims of negligence that do not involve physical harm to person or tangible property. Indeed, for at least a hundred years, Georgia courts have recognized that one whose negligence exposes others to a risk of ***criminal financial fraud*** cannot avoid liability if the risk was foreseeable and the instrumentality of harm was within the defendant's control. *E.g.*, *Atlanta Nat. Bank v. Bateman*, 94 S.E. 853, 855 (Ga. Ct. App. 1918); *Raleigh & G.R. Co. v. Lowe*, 28 S.E. 867, 868 (Ga. 1897) (“[W]here one of two innocent parties must suffer by the fraud of another, the loss should fall upon him who enabled such third person to commit the fraud.”).¹⁶

¹⁶ The principles underlying these cases refute Equifax's contention that

The authority above demonstrates that Georgia law does not categorically immunize defendants from the duty to act reasonably to avoid exposing others to the risk of criminal activity. The key to the analysis is foreseeability. *See Sun Trust Banks, Inc. v. Killebrew*, 464 S.E.2d 207, 211 (Ga. 1995) (Carley, J., concurring) (“If there is evidence of the occurrence of substantially similar prior criminal attacks *and* the knowledge of the proprietor thereof, then there is a jury question as to whether or not the proprietor had sufficient actual or constructive knowledge of an unreasonable risk of criminal attack so as to have the duty to exercise ordinary care to prevent a subsequent similar criminal attack.”).

In this case, Plaintiffs alleged numerous facts establishing that Equifax knew its actions could lead to a data breach and cause Plaintiffs harm. In its 2016 Form 10-K, Equifax acknowledged not only its obligation to protect consumer data, but there was a foreseeable risk that a data breach could occur and damage Equifax, consumers, and customers such as Plaintiffs. ¶133. Equifax is not a small,

Plaintiffs cannot recover because the compromised PII does not “belong” to Plaintiffs. *See* Br. at 31–33. While negligence claims involving data breaches differ from traditional “property loss” torts, Plaintiffs did not bring claims for trespass, bailment, or conversion, and a plaintiff’s ownership of property is not an element of a general negligence claim. Unlike chattel, PII can be reproduced, so exposing PII does not mean the PII has been “lost.” Instead, the harm comes through the destruction of the information’s exclusive association with an individual, and the resulting financial loss from identity theft. A negligence claim appropriately encompasses this pattern of harm – and Plaintiffs are the proper parties in interest – because Plaintiffs are the foreseeable victims of such harm.

unsophisticated company that stumbled its way into possessing millions of individuals' PII. Instead, Equifax's business is information. As a CRA, it intentionally collected and stored the PII of over 800 million individuals so it could sell this information, positioning itself as the linchpin of the consumer credit ecosystem. ¶¶107–09, 127. Equifax acknowledged that this data was highly valuable and constantly the target of hackers.¹⁷ Equifax knew and understood that the collection of such data required it to take proper measures to protect it, and that its failure to do so would lead to the damages Plaintiffs suffered.

Even before the Data Breach, Equifax acknowledged it was “regularly the target of attempted cyber and other security threats” and that it needed to be particularly vigilant against such attacks. ¶¶6, 133. Plaintiffs alleged that Equifax and its subsidiaries experienced at least five other data breaches compromising PII in the months leading up to the Data Breach. ¶¶150–55. At least three of those breaches involved criminal hacks. ¶¶152–54. In the same timeframe, numerous

¹⁷ Whether a defendant possessed or controlled property that was a tempting target for criminals is among the foreseeability factors that courts evaluate when determining the scope of the defendant's duty to protect against crime. ¶282; *see* RESTATEMENT (SECOND) OF TORTS, §302B cmts. e.(G.), f.; *see also* *Killebrew*, 464 S.E.2d at 209 (Sears, J., concurring) (identifying a probable jury question that a bank could reasonably anticipate criminal activity near ATMs, which pose tempting targets for criminals because customers use ATMs to withdraw cash). Here, Plaintiffs alleged Equifax's large collections of credit-related PII was an obvious target and should have been properly protected. ¶¶8, 137–42, 149.

independent entities criticized Equifax’s data security practices, including Equifax’s inadequate installation of security software patches. ¶¶156–64. Equifax even knew of the specific software vulnerability that ultimately led to the breach (¶¶176–81) but failed to act reasonably in response to the known risk. ¶¶180, 210–15. In the face of these allegations, the Court should resist Equifax’s claim for complete immunity from any duty to act reasonably under the circumstances.

Finally, Equifax pins blame for the Data Breach on the purportedly “unforeseeable” acts of criminals, Br. at 39, (that Equifax was aware of and specifically warned about (¶¶166-195)). Under Georgia law, this challenge cannot be resolved on a motion to dismiss unless “reasonable persons could not differ as to both the relevant facts and the evaluative application of legal standards (such as the legal concept of ‘foreseeability’) to the facts.” *Schernekau v. McNabb*, 470 S.E.2d 296, 298 (Ga. Ct. App. 1996); *see also Bishop v. Shorter Univ., Inc.*, No. 4:15-CV-00033-HLM (N.D. Ga. June 4, 2015), ECF No. 22, at 21-30 (attached as Exhibit B); *Ballenger Paving Co. v. Gaines*, 499 S.E.2d 722, 727 (Ga. Ct. App. 1998) (“If the original negligent actor reasonably could have anticipated or foreseen the intervening act and its consequences, then the intervening act of negligence will not relieve the original actor from liability”); *Warner*, 210 S.E.2d at 354 (“The immediacy of the connection between the inadequate

(although functioning) lock, the landlord’s notice of the inadequacy . . . compels us to hold that the landlord is not insulated as a matter of law, and that the jury should properly pass on the questions of agency, notice, foreseeability, intervening causation, assumption of risk, as well as the suitability of the lock in question.”). Because Equifax’s arguments seek to improperly resolve contested factual questions at the pleading stage, the Court should deny Equifax’s Motion.

2. Equifax Voluntarily Assumed a Duty to Handle Plaintiffs’ PII & PCD with Reasonable Care

Even if Equifax could claim that the foreseeability of a data breach did not give rise to a duty by Equifax to take reasonable preventative measures, under Georgia law, “[w]here one undertakes an act which he has no duty to perform and another reasonably relies upon that undertaking, the act must generally be performed with ordinary or reasonable care.” *Stelts v. Epperson*, 411 S.E.2d 281, 282 (Ga. Ct. App. 1991). Courts can find a voluntary undertaking even when the action was purely gratuitous and the allegations do not show that a formal contractual or fiduciary relationship was formed. *Id.*

Here, Equifax voluntarily assumed a duty to comply with applicable federal and state laws and protect the PII it collected. ¶¶124-34, 300–02, 331. Unlike the defendants in *Arby’s* and *Home Depot* that incidentally acquired PCD in the course of selling goods, Equifax’s primary business is collecting, aggregating, and selling

products and services containing sensitive, uniquely-identifying PII and PCD, which it obtains primarily from financial institutions and lenders. ¶¶103, 109–10, 335. As a linchpin of the consumer credit and reporting system, Equifax collects from and sells to Plaintiffs large volumes of PII. ¶¶99, 100, 102, 107. As Plaintiffs have alleged, the very nature of Equifax’s business places it in a special relationship with financial institutions. As a result, financial institutions relied on the security and accuracy of the PII in Equifax’s possession and used this PII to verify individuals’ identities and determine the credit worthiness of consumers. ¶¶105, 123, 136, 302, 353.

These detailed allegations are sufficient to establish that Equifax voluntarily assumed a duty to act reasonably when handling PII. It would be illogical (and contrary to Plaintiffs’ allegations) to assume that Equifax would not assume a duty to protect the PII it obtained from financial institutions. Accordingly, the Court should hold Equifax to the duty of care it publicly chose to assume.

B. Plaintiffs Alleged Causation and Damages

Echoing its arguments as to Article III standing, Equifax argues that Plaintiffs failed to allege the causation and damages elements of negligence because the alleged damages – resulting from Equifax’s actions in allowing customer data from approximately 147 million individuals to be breached – are too

attenuated or speculative. Br. at 35–41. For the reasons stated *supra* in Section I, these arguments ignore the factual allegations directly establishing the causation and damages elements of negligence. ¶¶10, 12-58, 234-61. *See Arby's I*, 2018 WL 2128441, at *10–11.

As in the question of duty, the limiting principle in the causation analysis is foreseeability, and the rationale underlying cases such as *Byrd v. English* is that a negligent act as to one person will typically not be considered the proximate cause of a third person's damaged contractual expectations. 43 S.E. 419, 420–21 (Ga. 1903); *see also* RESTATEMENT OF TORTS (Second), §766C & cmt. a (1979) (“In most of the cases in which recovery has been denied, the defendant has had no knowledge of the contract of prospective relation and no reason to foresee any harm to the plaintiff's interests”). Plaintiffs' allegations demonstrate that they were the directly foreseeable victims of a data breach and Equifax knew that a breach would directly harm Plaintiffs. In light of these allegations, the question of causation should be reserved for the jury. *Action Marine, Inc. v. Cont'l Carbon Inc.*, 481 F.3d 1302, 1310 (11th Cir. 2007).¹⁸

¹⁸ Equifax's reliance on *Collins v. Athens Orthopedic Clinic*, 815 S.E.2d 639 (Ga. Ct. App. 2018), to argue that Plaintiffs have failed to plead “any compensable damage” (Br. at 40-41), is misplaced. First, *Collins* is not binding on this Court. Ga. Ct. App. R. 33.2(a)(1). Second, *Collins* is factually distinguishable as the plaintiffs alleged only an “increased risk of harm” and potential future costs. 815

C. The Economic Loss Rule Does Not Apply

Equifax argues that Georgia's economic loss rule defeats Plaintiffs' negligence claim. Br. at 42. The *Arby's* and *Home Depot* courts held that Georgia's economic loss rule does not apply where a tort duty arises independently of any contractual obligation. *Arby's I*, 2018 WL 2128441, at *12–14; *Home Depot*, 2016 WL 2897520, at *3–4.

Equifax does not question this “independent duty exception,” but argues that *McConnell III* forecloses this Court from following *Arby's* and *Home Depot* and holding that Equifax owed a duty to the Plaintiffs. Br. at 42. For the reasons described above, *McConnell III* is distinguishable and does not compel a different outcome. When a defendant's actions create a foreseeable risk of harm, Georgia courts routinely permit negligence claims to proceed even if only a financial loss is involved. *See Construction Lender, Inc. v. Sutter*, 491 S.E.2d 853, 856 (Ga. Ct. App. 1997) (plaintiffs asserting negligence established that defendant voluntarily assumed a duty independent of contract and could recover funds improperly disbursed to contractor by lender); *Malak v. First Nat'l Bank of Atlanta*, 393

S.E.2d at 646. Based on those facts, the court held that “in the absence of some loss or damage,” the fact that data has been compromised “is not a compensable injury *by itself*.” *Id.* at 643. Unlike in *Collins*, Plaintiffs have alleged that they already have incurred actual losses resulting from the compromise of PII and PCD. *See supra* Section I. Thus, Plaintiffs have sufficiently alleged damages.

S.E.2d 267, 270 (Ga. Ct. App. 1990) (permitting action to be maintained against bank for negligently failing to honor a check, leading to foreclosure on plaintiff's property); *Bateman*, 94 S.E. at 855; *Lowe*, 28 S.E. at 868.

III. Plaintiffs State a Claim for Negligence Per Se

Plaintiffs assert a negligence per se claim premised on Equifax's violation of Section 5 of the Federal Trade Commission Act ("Section 5" or "FTC Act") and similar state statutes as well as the GLBA and 16 C.F.R. Part 314 (the "Safeguards Rule"). To establish negligence per se, a plaintiff must show that: (1) she is a member of the class the statute or regulation was intended to protect; (2) the injuries suffered were the kind the statute or regulation was enacted to prevent; and (3) the violation of the statute or regulation proximately caused these injuries. *See McLain v. Mariner Health Care, Inc.*, 631 S.E.2d 435, 437 (Ga. Ct. App. 2006). Further, the claim must be based on a statute or regulation that provides "some ascertainable standard of conduct." *Arby's I*, 2018 WL 2128441, at *7. "Where a statute provides a general rule of conduct, *although only amounting to a requirement to exercise ordinary care*, the violation thereof is negligence as a matter of law, or negligence per se." *Teague v. Keith*, 108 S.E.2d 489, 492 (Ga. 1959) (discussing that a negligence per se claim could be based on statutes prohibiting a driver from driving at a "speed greater than is reasonable," which was

“not too indefinite to furnish a rule of civil conduct”). Equifax’s admission that it must comply with the GLBA, Section 5, and similar state statutes demonstrates that these statutes and regulations necessarily have the force of law and impose ascertainable standards of conduct. ¶111 (Equifax admits “that it is ‘subject to numerous laws and regulations governing the collection, protection and use of consumer credit and other information, and imposing sanctions for the misuse of such information or unauthorized access to data,’” including the GLBA, Section 5, and state unfair trade practices acts) (quoting Equifax Inc., Annual Report (Feb. 22, 2017) at 3); *see also* ¶¶128-31. Equifax’s argument that these statutes cannot form the basis of this claim because neither the GLBA nor Section 5 provide for a private right of action (Br. at 47) is wrong. Georgia courts regularly find that statutes without a private right of action can form the basis for a claim of negligence per se. *See Bellsouth Telecomms., LLC v. Cobb Cty.*, 802 S.E.2d 686, 698 (Ga. Ct. App. 2017) (Dillard, P.J., concurring), *reconsideration denied* (July 12, 2017), *cert. granted* (Apr. 16, 2018) (rejecting similar argument, citing cases); *McLain*, 631 S.E.2d at 438; *Kull v. Six Flags Over Georgia II, L.P.*, 592 S.E.2d 143, 146 (Ga. Ct. App. 2003). As discussed below, Section 5 with the Federal Trade Commission’s (“FTC”) directives and the GLBA with the Safeguards Rule

provide a basis to allege a negligence per se claim.¹⁹

A. Section 5 and Similar State Statutes Provide a Basis for Plaintiffs’ Negligence Per Se Claim

Maintaining data security measures that are unreasonable and insufficient to safeguard confidential consumer information is an unfair practice under Section 5, as well as under the similar state statutes that are based on Section 5.²⁰ *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015); *In the Matter of LabMD, Inc.*, No. 9357, 2016 WL 4128215, at *10-13, 23 (F.T.C. July 28, 2016), *reversed on other grounds*, *LabMD, Inc. v. F.T.C.*, 894 F.3d 1221 (11th Cir. 2018). Although Equifax acknowledges that its security measures are subject to Section 5 of the FTC Act (¶¶128-29), Equifax argues that Section 5 “is not specific enough” to support this claim. Br. at 46. To the contrary, like in *Home Depot*, *Arby’s*, and *Wendy’s*, Plaintiffs adequately allege Equifax violated Section 5 by not having

¹⁹ Equifax also argues that Plaintiffs fail to allege that violation of these statutes proximately caused their injuries. Br. at 48-49. Plaintiffs addressed this argument in Section II above. Importantly, whether violation of a statute proximately caused the alleged injuries is a jury question. *See Lee v. Rodriguez*, No. 3:06-CV-083-JTC, 2008 WL 11417307, at *3 (N.D. Ga. June 24, 2008).

²⁰ Equifax claims Plaintiffs have failed to identify these statutes. Br. at 48 n.17. Plaintiffs identified the statutes that are based on the FTC Act (*see, e.g.*, ¶¶390, 403, 426, 454, 523, 592) and/or otherwise require Equifax to act reasonably in the management of PII and to use reasonable security measures to protect such data (*see, e.g.*, ¶¶366(c), 407(c), 528(c)) and specifically incorporates those statutes into the negligence per se claim. ¶317. The same rationale that supports Plaintiffs’ claim under Section 5 supports a claim under these statutes.

reasonable data security; Plaintiffs are within the class the statute was intended to protect; and the statute was meant to protect against the harm that occurred. ¶¶318-22; *Home Depot*, 2016 WL 2897520, at *4; *Arby's I*, 2018 WL 2128441, at *7-8; *First Choice Federal Credit Union v. Wendy's Co.*, No. 16-506, 2017 WL 9487086, at *4 (W.D. Pa. Feb. 13, 2017); *see also Bans Pasta, LLC v. Mirko Franchising, LLC*, No. 7:13-cv-00360, 2014 WL 637762, at *13-14 (W.D. Va. Feb. 12, 2014) (applying Georgia law and finding plaintiff adequately pleaded negligence per se based on FTC Act); *Legacy Acad., Inc. v. Mamilove, LLC*, 761 S.E.2d 880, 892 (Ga. Ct. App. 2014) (same), *vacated on other grounds*, 777 S.E.2d 731 (Ga. Ct. App. 2015).

Equifax misapplies *LabMD, Inc. v. FTC*, 894 F.3d 1221 (11th Cir. 2018), to argue Georgia common law does not support the finding of a duty under Section 5.²¹ Br. at 46-47. The *LabMD* Court explained that “[t]he **Commission** must find the standards of unfairness it enforces in . . . the Constitution, statutes, or the

²¹ The argument that Georgia common law does not support the finding of a duty in this case is incorrect for the independent reasons discussed above. *See supra* Section II (distinguishing *McConnell III*). Regardless, Section 5 is a federal statute and, as such, applies uniformly throughout the nation consistent with FTC and federal court interpretations of the FTC Act. To adopt Equifax’s rationale would render Section 5 and the FTC’s interpretations of the FTC Act subservient to the common law of the state in which the conduct at issue occurred, a dubious proposition for which Equifax provides no authority. *Cf.* U.S. Const. art. VI.

common law.” *LabMD*, 894 F.3d at 1231. Because the *LabMD* Court inferred that the common law was “the source of the standard of unfairness [the *Commission*] used in holding that LabMD’s failure to implement and maintain a reasonably designed data-security program constituted an unfair act or practice,” *id.*, Equifax wrongly concludes that Georgia common law necessarily can be the only source of the duty on which *Plaintiffs* can rely. This conclusion ignores that Plaintiffs may rely on Section 5 as the FTC has interpreted it through publications and enforcement orders.²² In passing the FTC Act, Congress specifically eschewed the idea of legislating the scope of acts that are unfair through the issuance of regulations; instead, it authorized the FTC to define “unfair acts or practices through case-by-case litigation.” *LabMD*, 894 F.3d at 1232. Thus, “once an act or practice is adjudged to be unfair, the act or practice becomes in effect—like an FTC-promulgated rule—an addendum to Section 5(a).” *Id.*; see also *In re TJX*

²² See ¶294 n.164 (FTC, Protecting Personal Information: A Guide for Business (Oct. 2016)); FTC, Start with Security: A Guide for Business (June 2015) (available at <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>) (citing FTC enforcement actions against businesses that fail to adhere to required security measures); *In the Matter of Credit Karma, Inc.*, No. 132-3091, 2014 WL 4252397, at *3-5 (FTC Aug. 13, 2014) (alleging Credit Karma misrepresented the security of customer information and violated Section 5 by failing to validate SSL certificates); *F.T.C. v. Lifelock Inc.*, No. 10-cv-00530, 2010 WL 1944122 (D. Ariz. Mar. 9, 2010), Complaint at ¶¶19-20, 35-36 (alleging LifeLock misrepresented the security of customers’ information in violation of Section 5 when it failed to install patches and encrypt and limit access to PII).

Cos. Retail Sec. Breach Litig., 564 F.3d 489, 496-97 (1st Cir. 2009) (finding FTC complaints and consent decrees instructive). Georgia law also does not require that a governmental directive be expressed in a statute or regulation to be enforceable. *See Wells Fargo Bank, N.A. v. Jenkins*, 744 S.E.2d 686, 688 (Ga. 2013) (recognizing negligence per se can be based on a “regulation, directive, or standard” authorized by law). Thus, Section 5, as interpreted by the FTC and courts, provides an ascertainable standard of conduct, and Equifax’s arguments must be rejected.

B. The GLBA with the Safeguards Rule Provides a Basis for Plaintiffs’ Negligence Per Se Claim

The failure to maintain reasonable data security measures to safeguard confidential consumer information in conformance with 16 C.F.R. Part 314 is a violation of the GLBA. *See In the Matter of Taxslayer, LLC*, No. 162-3063, 2017 WL 5477619, at *2 (F.T.C. Oct. 20, 2017) (enjoining Safeguards Rule violations where FTC alleged Taxslayer failed to assess reasonably foreseeable risks and to implement reasonable data security measures); *In the Matter of Taxslayer, LLC*, No. 162-3063, 2017 WL 5477618, at *4-5 (F.T.C. Oct. 20, 2017); *In the Matter of Paypal, Inc.*, No. 162-3102, 2018 WL 1182195, at *1, 3-4 (F.T.C. Feb. 27, 2018) (prohibiting misrepresentations and enjoining Safeguards Rule violations where FTC alleged Paypal misrepresented that it protected PII with “bank grade security

systems” and failed to assess reasonably foreseeable risks and to implement reasonable data security measures); *In the Matter of Paypal, Inc.*, No. 162-3102, 2018 WL 3046375, at *6, 9-11 (F.T.C. May 23, 2018). The Court should reject Equifax’s assertion that “Plaintiffs do not provide a single factual allegation that Equifax violated” the GLBA and the Safeguards Rule. Br. at 46. Plaintiffs specifically allege that Equifax violated 16 C.F.R. §314.4(b)-(c) because its data security measures were not adequate to: identify reasonably foreseeable risks, assess the sufficiency of any measures in place to control for these risks, or to detect, prevent, or respond to a data breach. ¶¶181-85, 203-07, 208-13, 219-22, 313. Equifax also violated 16 C.F.R. §314.4(e) because its data security measures were inadequate to evaluate and adjust to events that would have a material impact on Equifax’s information security program, such as the numerous prior data breaches that other retailers and Equifax itself had experienced (¶¶137-65, 313) and the notification to Equifax that an identified vulnerability in the Apache Struts software program it utilized would make Equifax particularly susceptible to a data breach. ¶¶173-80, 313.

Plaintiffs also allege that they are governed by the GLBA and the Safeguards Rule, and thus, are within the class intended to be protected and that the harm that has occurred is the type of harm the GLBA was intended to guard

against. ¶¶121, 315-16; *supra* Section I.A.1.b. As explained in *In re Bates*, No. 09-51279-NPO, 2010 WL 2203634, at *17 (Bankr. S.D. Miss. May 27, 2010), the GLBA:

was enacted “to enhance competition in the financial services industry” by allowing banks and other financial service providers to affiliate with one another and to allow those affiliated institutions to share confidential customer data. To allay concerns about maintaining the privacy of consumers notwithstanding the free-flow of information between merged financial service providers, the GLBA includes a privacy [and security] obligation policy[.]

See also New York State Bar Ass’n v. FTC, 276 F. Supp. 2d 110, 111 (D.D.C. 2003). In short, the “GLBA prescribes how financial institutions may share customer information” with each other. *Bates*, 2010 WL 2203634, at *17. To further the GLBA’s goals, the Safeguards Rule was implemented and it “applies to all customer information in [Equifax’s] possession, regardless of whether such information pertains to individuals with whom [it has] a customer relationship, or *pertains to the customers of other financial institutions [like many Plaintiffs and Class members] that have provided such information to [Equifax].*” 16 C.F.R. §314.1(b). Indeed, the information provided by financial institutions, like Plaintiffs, to CRAs, like Equifax, must be protected at every level. ¶315 (citing Interagency Guidelines Establishing Information Security Standards). Plaintiffs also are the entities that are required to reimburse consumers to the extent

consumers' financial accounts are impacted by identity theft or other fraudulent banking activity as a result of the Equifax Data Breach. *Id.* And, many Plaintiffs are credit unions that are organized as "member-owned" cooperatives whose members are the very consumers whose PII was compromised as a result of the Data Breach. *Id.* For these reasons, Plaintiffs are within the class intended to be protected, and the harm that has occurred is the type of harm the GLBA and the Safeguards Rule were intended to guard against.

Contrary to Equifax's argument, the GLBA with the Safeguards Rule provides an ascertainable standard of conduct. *Cf. Owens v. Dixie Motor Co.*, No. 5:12-CV-389-FL, 2014 WL 12703392, at *11, 14 (E.D.N.C. Mar. 31, 2014) (denying motion for summary judgment on claim of negligence per se for failure to comply with the GLBA); *Bates*, 2010 WL 2203634, at *16-18 (same); *Nicholas Homes, Inc. v. M & I Marshall & Ilsley Bank, N.A.*, No. CV09-2079-PHX-JAT, 2010 WL 1759453, at *3 (D. Ariz. Apr. 30, 2010) ("[A]lthough the GLBA does not provide for a private cause of action, it also does not preclude a common law cause of action"). *Jenkins*, which held that the GLBA does not articulate an ascertainable standard of conduct, 744 S.E.2d at 688, does not require a contrary result. Instead, the Georgia Supreme Court concluded a standard of conduct could only be found in the GLBA's implementing regulations, and since "[t]here is no

finding by the Court of Appeals of a violation of any regulation, directive, or standard,” the plaintiff failed to support her negligence claim. *Id.* at 688 & n.3. Unlike in *Jenkins*,²³ Plaintiffs expressly rely on the Safeguards Rule to articulate an ascertainable standard of conduct. ¶¶287-91. Thus, the GLBA and the Safeguards Rule are a sufficient basis for this claim.²⁴

IV. Plaintiffs State a Claim for Negligent Misrepresentation

To state a claim for negligent misrepresentation, a plaintiff must allege: (1) the defendant negligently supplied false information to foreseeable persons, known or unknown; (2) such persons reasonably relied upon that information; and (3) economic injury proximately resulted from that reliance. *See Higgins v. Bank of Am., N.A.*, No. 1:15-CV-01119, 2015 WL 12086083, at *3 (N.D. Ga. Sept. 22, 2015), *R&R adopted*, 2015 WL 12086093 (N.D. Ga. Oct. 20, 2015); *Robert & Co.*

²³ *See Jenkins v. Wachovia Bank N.A.*, No. 09C57922, 2010 WL 10063830 (Ga. St. Ct., Gwinnett Cty. Sept. 21, 2010), First Amended Complaint (failing to cite Safeguards Rule); *Jenkins v. Wachovia Bank N.A.*, No. A11A2053, 2013 WL 6836900, at *2 (Ga. App. Ct. Aug. 20, 2013), Supplemental Brief of Appellee Wells Fargo Bank, N.A. (stating plaintiff failed to raise Safeguards Rule as source of alleged duty until she filed surreply brief before the Georgia Supreme Court).

²⁴ The foregoing statutes and regulations also are illustrative of the standards of reasonable care relevant to establishing negligence. *See Laroche v. CSX Transport., Inc.*, No. CV 5 13-86, 2015 WL 5179011, at *4 (S.D. Ga. Sept. 3, 2015); *In re Killian*, No. ADV. 08-80250-HB, 2009 WL 2927950, at *8 (Bankr. D.S.C. July 23, 2009) (finding the GLBA a source of “a duty to refrain from placing the Killians’ personal information on the public record”).

Assocs. v. Rhodes-Haverty P'ship, 300 S.E.2d 503, 504 (Ga. 1983) (citing RESTATEMENT (SECOND) OF TORTS, §552 (1977)).²⁵

Plaintiffs allege that Equifax served as a trusted steward and linchpin of the credit reporting and verification system by representing that it understood data security and took necessary steps to safeguard PII. ¶¶97-110, 124-25, 132-33. Relying on these representations, Plaintiffs understood that Equifax would also maintain the accuracy and integrity of the data. *Id.* Having represented that it understood the need to secure PII and provide accurate and reliable information to financial institutions, and also having held itself out as a leader in cybersecurity, Equifax had a duty to ensure that these representations were current, accurate, and truthful. Equifax's failure to do so gives rise to a claim for negligent misrepresentation. *See Am. Casual Dining, L.P v. Moes' Southwest Grill, L.L.C.*, 426 F. Supp. 2d 1356, 1366 (N.D. Ga. 2006).

Equifax ignores Plaintiffs' allegations and asks the Court to hold that Plaintiffs have pleaded insufficient facts. However, Plaintiffs plead specific representations in which Equifax (i) held itself out as a leader and expert in

²⁵ In this District, "[t]here is no heightened pleading requirement to state a claim for negligent misrepresentation." *Higgins*, 2015 WL 12086083, at *4; *Atwater v. Nat'l Football League Players Ass'n*, No. CIVA 1:06CV1510 JEC, 2007 WL 1020848, at *13-14 (N.D. Ga. Mar. 29, 2007) (collecting cases). Regardless, Plaintiffs' allegations satisfy both Rule 8 and Rule 9(b).

anticipating and combatting cybersecurity threats, and (ii) made specific representations that it would comply with federal law and industry data security protocols to ensure that the PII was secure, including the following representations:

- “Furnishers who report data to Equifax play a vital role in helping identify credit risk and reduce financial losses throughout the entire credit granting community.” ¶124.
- Equifax is a “trusted steward of credit information for thousands of financial institutions and businesses, and millions of consumers. *We take this responsibility seriously, and follow a strict commitment to data excellence that helps lenders get the quality information they need to make better business decisions*” and “follow[s] a strict commitment to data excellence that helps lenders get the quality information they need to make better business decisions.” ¶125.
- “What’s more, in today’s environment of increasingly complex data privacy and security regulations, we provide businesses with more peace of mind and confidence when it comes to data reporting, and expert security compliance teams who are dedicated to data protection.” *Id.*
- Equifax is “continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives, while simultaneously delivering security for our services.” ¶127.
- Equifax devotes “substantial compliance, legal and operational business resources to facilitate compliance with applicable regulations and requirements” and has made a “substantial investment in physical and technological security measures.” ¶130.
- “We are committed to protecting the security of your personal information and use technical, administrative and physical security measures that comply with applicable federal and state laws.” ¶131.

- Equifax has “security protocols and measures in place to protect the personally identifiable information . . . and other information maintain[ed] about you from unauthorized access or alteration. These measures include internal and external firewalls, physical security and technological security measures, and encryption of certain data.” ¶132.
- “We collect and store sensitive data, including intellectual property, proprietary business information and personally identifiable information of our customers, employees, consumers and suppliers, in data centers and on information technology networks. The secure and uninterrupted operation of these networks and systems, and of the processing and maintenance of this information, is critical to our business operations and strategy.” ¶133.

Plaintiffs further detail how Equifax negligently supplied false information to Plaintiffs about its security measures given the scale and complexity of its business and massive volume of PII with which it was entrusted. ¶¶151-64. Indeed, as a result of the multiple data breaches Equifax experienced in the months preceding the Data Breach, Equifax knew or should have known that its data security measures were deficient. ¶¶151-55. That independent entities identified specific flaws in Equifax’s security protocols should have further led Equifax to know that its data security measures were deficient. ¶156. These independent entities specifically identified several deficiencies, including Equifax’s reliance on antiquated software, its failure to perform basic maintenance or install software patches. ¶¶157-64. Equifax conceded that it was aware of the Apache Struts

vulnerability in March 2017, and that it knew that patches for the vulnerability were available. ¶¶179-80; *see also* ¶¶208-15 (detailing findings of post-breach investigations and Equifax’s data security deficiencies). Thus, Plaintiffs sufficiently pleaded that Equifax knew or should have known that its data security practices were inadequate and not as represented.

As alleged, Equifax knew that Plaintiffs would rely on Equifax’s representations, because no reasonable financial institution would provide PII to Equifax or rely on the accuracy of Equifax’s data if it didn’t believe that Equifax was maintaining the highest level of security reasonably attainable by a “trusted steward” of data. At the time these statements were made, Equifax acknowledged that security threats and/or the loss of data were risk factors to its business, stating “[w]e rely extensively upon data from external sources to maintain our proprietary and non-proprietary databases, including data received from customers, strategic partners and various government and public record sources.” ¶¶126, 133. At the same time, Equifax held itself out as a data security expert and businesses relied on the accuracy and integrity of the information. ¶¶134-36. Building off of its reputation and representations regarding data security, Equifax developed and sold “data breach solutions” to financial institutions like Plaintiffs. ¶¶143-49. Thus, Equifax held itself out as a leader and expert in identifying and combatting

cybersecurity threats and fostered Plaintiffs’ reliance on its specialized knowledge, experience, and technologies.

Plaintiffs allege that they were justified in relying on the statements. ¶¶105, 123, 136. To the extent Equifax claims that Plaintiffs have not sufficiently pleaded justifiable reliance, such challenges are generally a question of fact that should not be resolved on a motion to dismiss. *Hendon Properties, LLC v. Cinema Dev., LLC*, 620 S.E.2d 644, 650 (Ga. Ct. App. 2005). Plaintiffs allege the necessary elements of this claim and the special relationship and the interconnectedness between Equifax and Plaintiffs, detailing how the foundation of Plaintiffs’ credit and financial services is grounded in Equifax’s management of consumer data. ¶¶97-106, 283. These factual allegations sufficiently plead a plausible basis for justifiable reliance. As discussed above in Sections I-II, Plaintiffs also alleged cognizable injuries proximately caused by Equifax’s conduct. Thus, Equifax’s Motion should be denied.

V. Plaintiffs Adequately Allege Their State Statutory Claims

A. Plaintiffs Can Constitutionally Bring Non-Georgia Statutory Claims against Equifax

Equifax’s constitutional attack on Plaintiffs’ non-Georgia statutory claims must be rejected under well-recognized Supreme Court precedent. The “long accepted” constitutional rule is “that a set of facts giving rise to a lawsuit, or a

particular issue within a lawsuit, may justify, in constitutional terms, application of the law of more than one jurisdiction.” *Allstate Ins. Co. v. Hague*, 449 U.S. 302, 308 (1981). Despite this rule, Equifax claims Plaintiffs’ non-Georgia statutory claims cannot be applied “extraterritorially” because, according to Equifax, *all* the wrongful conduct occurred in Georgia. Br. at 55. Equifax’s argument ignores Plaintiffs’ factual allegations and mischaracterizes the relevant case law.

Contrary to Equifax’s claims, Plaintiffs allege Equifax committed its wrongful conduct in each state whose laws Plaintiffs invoke. Equifax is licensed to do and does business in all fifty states, both providing and receiving sensitive information and PII from Plaintiffs and the Class throughout the country. ¶¶107, 109, 110. Equifax misled Plaintiffs – who are residents of the states whose laws they invoke – about the quality of its data security measures and acted unfairly towards Plaintiffs by deliberately implementing woefully inadequate data security measures. ¶¶124-36. Equifax’s unlawful conduct furthermore caused Plaintiffs’ injuries in the states whose laws they invoke. ¶¶9-10, 12-84. Thus, the application of non-Georgia substantive law is neither arbitrary nor unfair under *Allstate* because the aggregation of contacts alleged creates a state interest in applying laws outside of Georgia’s. *See Allstate*, 449 U.S. at 307-13.

Equifax's cases do not hold otherwise.²⁶ *State Farm Mut. Ins. Co. v. Campbell*, 538 U.S. 408 (2003), strictly considered the appropriate proportion of punitive damages to actual damages. To the extent the Court discusses the constitutionality of imposing punitive damages on a defendant for its out-of-state conduct, the Court, and subsequent cases, hold such limitations exist only where the alleged out-of-state conduct does not cause plaintiff's injuries. *See id.* at 422. *See also Crouch v. Teledyne Cont'l Motors*, No. 10-00072-KD-N, 2011 WL 1539854, at *3-4 (S.D. Ala. Apr. 21, 2011) (*State Farm* does not apply where the "alleged out-of-state conduct resulted in injury to the Plaintiffs" in their home states). Here, Equifax's conduct in Georgia clearly contributed to the injuries Plaintiffs experienced in their home states, and thus application of non-Georgia

²⁶ Plaintiffs' facts distinguish *Flatirons Bank v. Alan W. Steinberg Ltd. P'ship*, 233 So.3d 1207, 1211 (Fla. Dist. Ct. App. 2017) and *Campbell v. Albers*, 39 N.E.2d 672, 676 (Ill. Ct. App. 1942), where the defendants did not commit any conduct in the states whose laws plaintiffs sought to impose on defendants, and *Bonaparte v. Tax Ct.*, 104 U.S. 592, 594 (1881), which held states cannot tax a *situs* that resides entirely in another state. In *Sawyer v. Market Am. Inc.*, 661 S.E.2d 750, 754 (N.C. Ct. App. 2008), the court held the state's labor laws were not enacted to protect non-residents, and therefore the plaintiff had no standing to sue under those laws. Here, Plaintiffs are residents of the states under whose laws they bring claims, and, therefore, *Sawyer* is inapplicable. *Healey v. Beer Ins.*, 491 U.S. 324 (1989), also is inapplicable because it did not consider the extraterritorial application of laws, but rather state discrimination against out-of-state activity by favoring and promoting in-state activity. *Id.* at 340-41. Equifax cannot show consumer protection statutes discriminate against out-of-state activity.

law is entirely constitutional.²⁷

B. Equifax Misstates the Elements Required for the Statutory Claims at Issue

1. Plaintiffs’ Statutory Claims Based on Equifax’s Unfair Conduct Need Not Meet All the Elements of Fraud

Equifax argues Plaintiffs have not adequately pleaded the elements of “fraud” with regard to their statutory claims. Br. at 57-58. However, “consumer protection claims are not claims of fraud, even if there is a deceptive dimension to them.” *Consumer Financial Protection Bureau v. RD Legal Funding, LLC*, No. 17-CV-890 (LAP), 2018 WL 3094916, at *21 (S.D.N.Y. June 21, 2018).²⁸ Furthermore, Equifax fails to recognize that half of Plaintiffs’ statutory claims are based on “unfair” rather than “deceptive” acts, and do not contain the traditional

²⁷ To the extent any doubt exists, the following cases involve the “extraterritorial” application of state law where the defendant committed the wrongful conduct in the state and harmed a resident plaintiff: *Rogers v. Omni Sol.*, No. 10-21588-CIV, 2010 WL 4136145, at *4 n.2 (S.D. Fla. Oct. 19, 2010) (FL); *Van Tassell v. United Mktg. Grp.*, 795 F. Supp. 2d 770, 781-82 (N.D. Ill. 2011) (IL); *Cruz v. FXDirectDealer*, 720 F.3d 115, 122 (2d Cir. 2013) (NY); *ITCO Corp. v. Michelin Tire*, 722 F.2d 42, 49 (4th Cir. 1983) (NC).

²⁸ Equifax argues Plaintiffs must meet the elements of fraud to adequately plead its consumer protection claims; but, the cases it cites deal with simple fraud claims and not consumer protection claims. Br. 57-58 (citing *Crespo v. Coldwell Banker Mortg.*, 599 F. App’x 868, 873 (11th Cir. 2014); *Rodi v. S. New England School of Law*, 532 F.3d 11, 16-17 (1st Cir. 2008); *Next Century Commc’ns Corp. v. Ellis*, 318 F.3d 1023, 1026-27 (11th Cir. 2003)).

elements of fraud. *See* Ex. A-1.²⁹ Equifax’s grossly overgeneralized argument is thus insufficient to warrant dismissal of Plaintiffs’ claims alleging unfair conduct.

To show that a defendant acted unfairly, these statutes examine whether the defendant’s conduct is “immoral, unethical, oppressive, unscrupulous, or substantially injurious,” “is attended by some reprehensible conduct,” or “offends public policy.” *See* Ex. A-1. Plaintiffs have sufficiently alleged that Equifax acted “unfairly” by compromising the credit reporting and verification system in violation of public policy. Plaintiffs allege that Equifax knew that financial institutions would be responsible for remedying and mitigating the consequences of a data breach. ¶¶111-23, 137-49, 237-39. Despite understanding the harm a breach would cause Plaintiffs, Equifax deliberately took inadequate measures to protect PII and PCD. ¶211 (“The Warren Report noted that despite record profits in recent years, Equifax spent only a fraction of its budget on cybersecurity.”); *see also* ¶¶124-26, 130-36. At the same time, Equifax prevented Plaintiffs from learning of its deficient data security measures by making affirmative misrepresentations about its data security. ¶¶124-36.³⁰ This Court has found that

²⁹ The charts that Plaintiffs submit concurrently herewith are in response to the case law cited in the chart Equifax submitted with its Motion. ECF No. 435-2.

³⁰ Equifax furthermore violated public policy as reflected in the GLBA, FCRA, the FTC Act, and state statutes that require businesses to safeguard PII and PCD.

relying on similarly unreasonable data security measures constitutes an unfair act. *Home Depot*, 2016 WL 2897520, at *5-7 (denying motion to dismiss statutory claims, including CUTPA, ICFA, and Chapter 93A claims); *see also In re Arby's Rest. Grp. Inc. Litig. (Arby's II)*, 317 F. Supp. 3d 1222, 1227-28 (N.D. Ga. 2018) (denying motion to dismiss GFBPA claim); *TJX*, 564 F.3d at 496 (denying motion to dismiss Chapter 93A claim based on FTC interpretations).³¹

2. Plaintiffs' Statutory Claims Based on Equifax's Deceptive Conduct Need Not Meet All the Elements of Fraud

As with the claims of unfair conduct, none of the statutes under which Plaintiffs bring claims rooted in Equifax's deceptive conduct require Plaintiffs to prove the strict elements of fraud. *See* Ex. A-2. Instead, Plaintiffs adequately plead Equifax violated each of the relevant statutes by making misleading statements about the reasonableness of its data security measures. Plaintiffs cite specific statements that Equifax made alleging that it was a "trusted steward" that complies with the laws requiring it to adequately safeguard consumer data. ¶¶124-¶¶349, 395, 409, 435, 448, 461, 505, 549, 575, 599. Equifax's acts thus violated public policy in the states where Plaintiffs bring claims based on Equifax's "unfair" conduct.

³¹ Each of the state statutes under which Plaintiffs allege Equifax acted unfairly incorporates the FTC's interpretations of prohibited unfair conduct. *See* Ex. A-1; *Home Depot*, 2016 WL 2897520, at *5 (looking to the FTC Act for guidance as to unfair conduct). *Wyndham* specifically held unreasonable data security measures, as those alleged by Plaintiffs, constitute "unfair" conduct under the FTC Act. *Wyndham*, 799 F.3d at 245-47.

36, 150-65. Plaintiffs allege that Equifax represented it was a “trusted data provider with industry-leading data security and protection protocols” and devoted “substantial investment in physical and technological security measures.” ¶¶125, 127. Equifax assured Plaintiffs they could have “peace of mind” because of Equifax’s “dedicat[ion] to data protection.” ¶125. Those representations were likely to mislead Plaintiffs into believing that Equifax had enacted reasonable, and in fact, top-of-the-line data security measures. ¶355. In reality, Equifax implemented unreasonable data security measures and never remediated known vulnerabilities. Equifax’s misrepresentations about its data security measures thus constitute deceptive conduct. *See Arby’s II*, 317 F. Supp. 3d at 1224, 1228 (denying motion to dismiss GFBPA claim where plaintiffs pled that “Arby’s had knowledge of the vulnerabilities in its data systems yet misrepresented itself to be compliant with data security protection standards”); *Wendy’s*, 2017 WL 9487086, at *4 (same as to Ohio Deceptive Trade Practices Act claim).

Finally, apart from “deceptive” and “unfair” conduct, Plaintiffs allege that Equifax’s acts constitute “unconscionable” conduct. *See* ¶¶366 (Arkansas Deceptive Trade Practices Act), 403 (Florida Deceptive and Unfair Trade Practices Act (“FDUTPA”), 530 (New Mexico Unfair Practices Act), 575 (Oklahoma Consumer Protection Act (“OCPA”). An unconscionable act is generally one that

“takes advantage of the lack of knowledge, ability, experience or capacity of a person to a grossly unfair degree.” N.M. Stat. Ann. §57-12-2 (E)(1); *see also Erbar v. Rare Hosp. Int’l, Inc.*, 316 P.3d 937, 942 (Okla. Ct. App. 2013) (similar); *Baptist Health v. Murphy*, 226 S.W.3d 800, 811 & n.6 (Ark. 2006) (unconscionable acts “affront the sense of justice, decency, or reasonableness,” and “includes conduct violative of public policy or statute.”); Fla. Stat. §501.204(1). Here, Equifax acted “unconscionably” because it represented to Plaintiffs that its data security measures were reasonable, taking took advantage of Plaintiffs’ inability to discover the true state of Equifax’s data security measures and remedy Equifax’s data security deficiencies. ¶¶124-36, 179-82. Plaintiffs had no opportunity to learn of Equifax’s deficient data security measures, and were later harmed because of them. Equifax’s conduct was thus unconscionable.

a. Plaintiffs Meet the Heightened Pleading Standard to the Extent Required

Rule 9(b)’s pleading standard generally does not apply to consumer protection statutes. *See, e.g., Consumer Financial Protection Bureau v. Frederick Hanna*, 114 F. Supp. 3d 1342, 1372-73 (N.D. Ga. 2015). Conceding that some claims are not subject to Rule 9(b), Br. at Ex-1; *see also* Ex. A-2, Equifax still seeks dismissal of *all* of Plaintiffs’ state statutory claims for failure to plead with particularity under Rule 9(b). To the extent particularity is required, it is satisfied

by Plaintiffs’ allegations regarding the contents of Equifax’s affirmative misrepresentations, where and to whom those misrepresentations were made, and why they were misleading. *Johannaber v. Emory Univ.*, No. 1:08-CV-2201-TWT, 2009 WL 10671453, at *1 (N.D. Ga. Dec. 14, 2009). Plaintiffs specifically quote Equifax’s public representations concerning the quality of its data security measures, including on its website. ¶¶124-36. Plaintiffs allege that these representations were misleading as evidenced by Equifax’s numerous prior data breaches and known security vulnerabilities. ¶¶151-65. Plaintiffs allege that, contrary to its representations, Equifax deliberately delayed remedying known data security vulnerabilities despite widespread concern that hackers would exploit them. ¶¶166-78. These allegations are sufficiently specific to put Equifax on notice of the misrepresentations at issue. *Hill v. Morehouse Med. Assocs., Inc.*, No. 02-14429, 2003 WL 22019936, at *3 (11th Cir. Aug. 15, 2003) (Rule 9(b) “may be applied less stringently . . . when specific factual information [about the fraud] is peculiarly within the defendant’s knowledge or control.”).

b. Plaintiffs Adequately Allege Scier to the Extent Required

Equifax argues that all but Counts 8 (FDUTPA), 15 (Minnesota Plastic Card Security Act (“MPCSA”)), and 19 (New York General Business Law (“N.Y. GBL”) §349) must be dismissed because Plaintiffs failed to plead sufficient facts

demonstrating that “Equifax knowingly violated any statute or intended to mislead Plaintiffs.”³² Br. at 59. Equifax cites no authority showing that scienter is an element of any claims, justifying denial of its Motion on that basis alone. *See* Ex. A-2. In any event, Plaintiffs specifically allege scienter by pleading facts showing Equifax’s knowledge and intent. *See, e.g.*, ¶¶124-36 (Equifax knowingly failed to disclose that its data security measures were deficient); ¶¶137-49 (Equifax understood it was a target of hackers and knew it was obligated to safeguard PII); ¶¶150-83 (Equifax intentionally deprioritized data security and knowingly ignored warnings from independent entities). These allegations are sufficient at this stage. *Miles Rich Chrysler-Plymouth*, 411 S.E.2d at 905; *Ruk v. Crown Asset Mgmt., LLC*, No. 1:16-CV-03444-LMM, 2017 WL 3085686, at *3 (N.D. Ga. June 8, 2017) (“Allegations of a negligent violation require a lower burden of proof regarding scienter than allegations for a willful violation.”).

³² Scienter does not require Equifax to have knowingly violated the statutes, as Equifax claims. Br. at 58. Rather, Equifax must have knowingly committed the alleged unfair or deceptive practices independent of whether Equifax knew such conduct was illegal. *See, e.g., Miles Rich Chrysler-Plymouth, Inc. v. Mass.*, 411 S.E.2d 901, 905 (Ga. Ct. App. 1991) (“The intentional violation as contemplated by the [GFBPA] is a volitional act constituting an unfair or deceptive act or practice conjoined with culpable knowledge of the nature (but not necessarily the illegality of the act).”).

c. Plaintiffs Adequately Allege Reliance to the Extent Required

To the extent reliance is required with respect to Plaintiffs' misrepresentation-based allegations (Ex. A-2), Plaintiffs have pleaded it. *See supra* Section IV. *Higgins*, 2015 WL 12086083, at *4.

3. Plaintiffs Adequately Allege Injury

As discussed above in Sections I-II, Plaintiffs have sufficiently alleged cognizable injuries proximately caused by Equifax's conduct. Equifax argues that Counts 5 (ADTPA), 7 (CUTPA), 8 (FDUTPA), 10 (ICFA), 11 (LUTPA), 18 (NMUPA), 19 (N.Y. GBL §349), and 24 (TCPA) should be dismissed because Plaintiffs failed to allege an injury that is both ascertainable and monetary. *Id.* Equifax ignores Plaintiffs' allegations, which specifically describe Plaintiffs' alleged out-of-pocket costs that are ascertainable and monetary. Ex. A-4.

4. Equifax Mischaracterizes Plaintiffs' Equitable Claims

Equifax misconstrues Plaintiffs' requested relief under the Minnesota and Nebraska Uniform Deceptive Trade Practices Acts. Br. at 60. Plaintiffs do not seek money damages under these statutes, but merely request "all monetary and non-monetary relief allowed by law." ¶¶489 (MN), and 521 (NE). Monetary relief in the form of attorneys' fees and/or costs is available under each statute. *See* Minn. Stat. §325D.45, subd. 2; N.R.S.A. §87-303(b). While the Nevada claim

inadvertently mentions “civil penalties,” that clause is rendered inoperative by the “allowed by law” caveat. ¶521. The Court should thus deny Equifax’s Motion.

5. Plaintiffs Qualify as “Consumers”

Equifax seeks dismissal of Counts 8 (FDUTPA), 10 (Illinois Consumer Fraud and Deceptive Business Practices Act), 13 (Minnesota Consumer Fraud Act), 19 (N.Y. GBL §349), 20 (North Carolina Unfair and Deceptive Trade Practices Act) and 22 (OCPA) because these statutes purportedly “only protect consumers, not businesses.” Br. at 60 & Ex. 1. Equifax is wrong. Each statute allows businesses to sue. Ex. A-3. To bring claims under these statutes, Plaintiffs must be a “consumer” of Equifax’s goods or services and/or Equifax’s deceptive conduct must have affected the market at large. Plaintiffs allege that they used and consumed Equifax’s services, which Equifax acknowledges. ¶131 (discussing Equifax’s “commitment to deliver reliable information to our customers (both businesses and consumers).”); ¶135 (acknowledging Equifax’s “products and services enable businesses to make credit and service decisions”); *see also* ¶¶1, 7, 109, 136. Additionally, Equifax’s unfair acts and misrepresentations undoubtedly impacted the marketplace. Equifax accumulated PII on hundreds of millions of individuals while exposing that PII to a substantial risk of a data breach. ¶¶107, 139. Plaintiffs, as consumers of such information, relied on the confidentiality and

authenticity of the information provided. ¶¶3, 5. Thus, Plaintiffs are entitled to sue under these statutes.

6. State-Law Class Action Bans Are Unenforceable.

Equifax concedes that “this Court is bound” by *Lisk v. Lumber One Wood Preserving, LLC*, 792 F.3d 1331 (11th Cir. 2015). Br. at 54 n.20. Thus, “Rule 23 applies in this case,” and state-law class action bans are unenforceable. *Lisk*, 792 F.3d at 1337, 1335-37; *Mounce v. CHSPSC, LLC*, No. 5:15-CV-05197, 2017 WL 4392048, at *7 (W.D. Ark. Sept. 29, 2017) (rejecting ADTPA class action ban); *In re Hydroxycut Mktg. & Sales Practices Litig.*, 299 F.R.D. 648, 652-54 (S.D. Cal. 2014) (same as to GFBPA, LUTPA, and TCPA class action bans).

C. Equifax’s Claim-Specific Arguments Lack Merit

1. *McConnell III* Is Irrelevant to Plaintiffs’ GFBPA Claim

Attempting to circumvent the GFBPA entirely, Equifax argues that if the GFBPA contained a duty to safeguard data, then *McConnell III* would not have dismissed the plaintiff’s negligence claim. *McConnell III*, however, did not consider a GFBPA claim at all, nor what constitutes “unfair” or “deceptive” conduct under Georgia law. *McConnell III* merely noted that the existence of a GFBPA provision not to “publicly post” social security numbers could not serve as the source for “a general duty to safeguard and protect” PII. 814 S.E.2d at 798.

Plaintiffs here, however, specifically plead that Equifax’s adoption of unreasonable data security measures constitutes an unfair and/or deceptive act that violates the GFBPA itself. ¶¶339-59. Thus, *McConnell III* has no application to Plaintiffs’ GFBPA claim.

2. Plaintiffs Can Enforce a Massachusetts Ch. 93A Claim

Massachusetts Chapter 93A unquestionably provides for a private right of action. Mass. Gen. Laws Ch. 93A, §11. A violation of M.G.L.A. c. 93H (“Chapter 93H”) can form the basis of a claim under Chapter 93A.³³ Unlike the plaintiff in *Katz v. Pershing*, 806 F. Supp. 2d 452, 458 (D. Mass. 2011) (Br. at 61), Plaintiffs sufficiently alleged a Chapter 93A violation without reliance on Chapter 93H. ¶¶459-61 (alleging unfair and deceptive conduct based on failure to comply with duties under the common law, FTC Act, FCRA, and GLBA and misrepresenting it would protect PII and comply with its duties). These allegations are sufficient at this stage. *Home Depot*, 2016 WL 2897520, at *6 & n.88.

³³ Violation of a statute or regulation may constitute an unfair practice under Chapter 93A. See *Klaimont v. Gainsboro Rest., Inc.*, 987 N.E.2d 1247, 1255 (Mass. App. Ct. 2013). The statute providing the basis for the Chapter 93A claim need not contain a private right of action. See *Hershenow v. Enterprise Rent-A-Car Co. of Boston, Inc.*, 840 N.E.2d 526, 531-32 (Mass. 2006); see also *Adams v. Cong. Auto Ins. Agency, Inc.*, 65 N.E.3d 1229, 1239 (Mass. App. Ct. 2016), review denied, 86 N.E.3d 243 (Mass. 2017) (implicitly recognizing a Chapter 93A claim predicated on Chapter 93H).

3. Plaintiffs Adequately Allege the MPCSA Claim

Equifax argues Plaintiff Firefly Credit Union's ("Firefly") claim under the MPCSA fails because "Firefly has not alleged that Equifax improperly maintained" the data covered by the MPCSA (*i.e.*, CVV codes, PIN verification numbers, and magnetic stripe data), *see* Minn. Stat. §325E.64, subd. 2, "for any card that it issued." Br. at 61. This argument must be rejected. *See supra* Section I.A.1.c. Firefly specifically alleges that Equifax "retain[ed] payment card data (the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data) longer than allowed by the statute," ¶495, and that Firefly "received fraud alerts from one or more of the payment card brands identifying payment cards it issued that were compromised in the Equifax Data Breach." ¶496. Plaintiffs also allege that the card brand alerts identified that data protected by the MPCSA was compromised. ¶¶187-88. When read together, Firefly sufficiently alleges that Equifax violated the MPCSA as to the cards it issued. *Home Depot*, 2016 WL 2897520, at *7; *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1314 (D. Minn. 2014).

VI. *Schnuck Markets* Is Inapposite

Equifax argues that *Comm. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803 (7th Cir. 2018) requires dismissal of the claims related to compromised

payment cards. Br. at 62–64. This argument has no merit because the present case lacks the crucial fact upon which *Schnuck Markets* turned: the plaintiffs **and** the defendant there were involved in a network of contracts that determined the duties imposed and remedies available for breaches of those duties. 887 F.3d at 814 (“plaintiff banks and Schnucks **all** participate in a network of contracts...”). The Seventh Circuit found this fact dispositive in determining that under Illinois and Missouri law, the economic loss rule barred plaintiffs’ negligence claims. *Id.* at 816–18.

Here, Plaintiffs did not allege that Equifax was contractually involved in payment card networks, and Equifax does not suggest that it is. Instead, Equifax notes only that Plaintiffs apparently have agreements with the card brands. Br. at 63–64. But without some contractual link running **between Plaintiffs and Equifax**, *Schnuck Markets* is inapplicable; the Seventh Circuit acknowledged as much when it specifically stated that the Equifax data breach presented a fundamentally different scenario. *Schnuck Markets*, 887 F.3d at 815 (“This is also not a situation where sensitive data is collected and then disclosed by private, third-party actors who are not involved in the customers’ or banks’ direct transactions”) (citing *In re Equifax, Inc., Customer Data Security Breach Litig.*, 289 F. Supp. 3d 1322 (J.P.M.L. 2017)).

Moreover, Equifax is wrong to suggest that the Seventh Circuit's interpretation of Illinois and Missouri law can be applied on the basis that Georgia law is purportedly "indistinguishable." Br. at 64. In *Arby's* and *Home Depot*, this Court, and another in this District, analyzed the same payment card network relationships at issue in *Schnuck Markets*, and in both cases determined that Georgia's economic loss doctrine did not bar a negligence claim where the plaintiff adequately alleged breach of a duty arising independently of the contractual relationships. *See Arby's I*, 2018 WL 2128441, at *12–14; *Home Depot*, 2016 WL 2897520, at *3. Because this Court should likewise find that Equifax was under a non-contractual duty to handle PCD with reasonable care (*see supra* Section II.A), Equifax's invocation of *Schnuck Markets* should be rejected.

VII. Plaintiffs Adequately Allege Their Entitlement to Equitable Relief³⁴

Plaintiffs seek a declaration of rights and ancillary injunctive relief pursuant to 28 U.S.C. §2201, *et seq.*, in light of the substantial controversy that exists relating to Equifax's ongoing data security obligations. *See MedImmune, Inc. v.*

³⁴ Equifax's argument that Plaintiffs' request for attorneys' fees should be dismissed (Br. at 65 n.28) is meritless. Plaintiffs have stated their claims and thus would be entitled to attorneys' fees under the state statutory claims alleged. *See, e.g.*, ¶358; O.C.G.A. §10-1-399(d); *Campbell v. Beak*, 568 S.E.2d 801, 804, 806-07 (Ga. Ct. App. 2002) (plaintiff awarded attorney's fees under the GFBPA without pleading O.C.G.A. §13-6-11). In any event, Plaintiffs can amend their Complaint to specifically seek attorneys' fees under this statute.

Genentech, Inc., 549 U.S. 118, 127 (2007); *Powell v. McCormack*, 395 U.S. 486, 499 (1969). Plaintiffs allege Equifax’s current data security practices remain inadequate, which Equifax denies. ¶¶607, 610; Br. at 65-66. Plaintiffs further allege there is a real, immediate, and substantial risk of another data breach and resultant future harm for which Plaintiffs will not have an adequate legal remedy. ¶¶610-11; *see also* ¶¶150-56. Such allegations are sufficient at the pleading stage. *See Home Depot*, 2016 WL 2897520, at *4-5; *Arby’s I*, 2018 WL 2128441, at *14-15; *Wendy’s*, 2017 WL 9487086, at *5.

Equifax’s arguments for dismissal lack merit. First, regardless of whether Plaintiffs have adequately stated their substantive claims, Plaintiffs satisfy the “actual controversy” requirement to obtain declaratory relief. *See* 28 U.S.C. §2201; *Aetna Life Ins. Co. of Hartford, Conn. v. Haworth*, 300 U.S. 227, 239-40 (1937); ¶¶607, 610. Second, Equifax’s argument that Plaintiffs fail to allege that they “continue to be harmed by any ongoing failures in Equifax’s data-security practices,” Br. at 66, ignores Plaintiffs’ allegations, ¶¶233-34, 237, 244, 607, 610; *see also* ¶¶150-56, and impermissibly raises a factual dispute that is premature at this stage. *Arby’s I*, 2018 WL 2128441, at *15. Finally, Equifax’s invocation of *LabMD* to argue the requested injunctive relief is unenforceable is also premature. Plaintiffs can tailor a proposed order to pass muster under *LabMD* (which was

entered after the Complaint was filed) at the appropriate juncture in the case.

CONCLUSION

For the foregoing reasons, the Court should deny Equifax's Motion.

Respectfully submitted this 20th day of September, 2018.

/s/ Joseph P. Guglielmo

Joseph P. Guglielmo

**SCOTT+SCOTT ATTORNEYS AT
LAW LLP**

230 Park Avenue, 17th Floor

New York, New York 10169

Tel. 212.223.6444

jguglielmo@scott-scott.com

Gary F. Lynch

**CARLSON LYNCH SWEET KILPELA
& CARPENTER, LLP**

1133 Penn Avenue, 5th Floor

Pittsburgh, Pennsylvania 15222

Tel. 412.322.9243

glynch@carsonlynch.com

***Financial Institution Plaintiffs' Co-Lead
Counsel***

Craig A. Gillen

GILLEN WITHERS & LAKE, LLC

3490 Piedmont Road, N.E.

One Securities Centre, Suite 1050

Atlanta, Georgia 30305

Tel. 404.842.9700

cgillen@gwilllawfirm.com

MaryBeth V. Gibson

THE FINLEY FIRM, P.C.

3535 Piedmont Road
Building 14, Suite 230
Atlanta, Georgia 30305
Tel. 404.320.9979
mgibson@thefinleyfirm.com

Ranse Partin

CONLEY GRIGGS PARTIN LLP

4200 Northside Parkway
Building One, Suite 300
Atlanta, Georgia 30327
Tel. 404.572.4600
ranse@onleygriggs.com

***Financial Institution Plaintiffs' Co-Liaison
Counsel***

Arthur M. Murray

MURRAY LAW FIRM

650 Poydras Street, Suite 2150
New Orleans, Louisiana 70130
Tel. 504.525.8100
amurray@murray-lawfirm.com

Stacey P. Slaughter

ROBINS KAPLAN LLP

800 LaSalle Avenue, Suite 2800
Minneapolis, Minnesota 55402
Tel. 612.349.8500
sslaughter@robinskaplan.com

Charles H. Van Horn

BERMAN FINK VANHORN P.C.

3475 Piedmont Road, Suite 1100
Atlanta, Georgia 30305
Tel. 404.261.7711
cvanhorn@bfvlaw.com

Allen Carney
CARNEY BATES & PULLIAM, PLLC
519 W. 7th Street
Little Rock, Arkansas 72201
Tel. 501.312.8500
acarney@cbplaw.com

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
17 Washington Avenue North
Suite 300
Minneapolis, Minnesota 55401
Tel. 612.339.7300
bbleichner@chestnutcambronne.com

Karen Hanson Riebel
**LOCKRIDGE GRINDAL NAUEN
P.L.L.P.**
100 Washington Ave. S., Suite 2200
Minneapolis, Minnesota 55401
Tel. 501.812.5575
khriebel@locklaw.com

Karen S. Halbert
ROBERTS LAW FIRM, PA
20 Rahling Circle
P.O. Box 241790
Little Rock, Arkansas 72223
Tel. 501.821.5575
karenhalbert@robertslawfirm.us

Brian C. Gudmundson
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, Minnesota 55402
Tel. 612.341.0400

brian.gudmunson@zimmreed.com

***Financial Institution Plaintiffs' Steering
Committee***

CERTIFICATE OF COMPLIANCE

Pursuant to L.R. 7.1D, the undersigned certifies that the foregoing complies with the font and point selections permitted by L.R. 5.1B. This Response was prepared on a computer using the Times New Roman font (14 point).

Respectfully submitted this 20th day of September, 2018.

/s/ Joseph P. Guglielmo
Joseph P. Guglielmo

CERTIFICATE OF SERVICE

I hereby certify that on September 20, 2018, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Joseph P. Guglielmo
Joseph P. Guglielmo